LOS DELITOS INFORMATICOS RELATIVOS A LA INTIMIDAD, LOS DATOS PERSONALES Y EL HABEAS DATA EN EL DERECHO COLOMBIANO

Por: Libardo Orlando Riascos Gómez (*)

I. LOS DELITOS INFORMATICOS CONTRA BIENES JURIDICOS INTANGIBLES: 1. Notas preliminares. 2. Regulación iuspenalista del derecho de acceso a la información, el habeas data y la intimidad. 3. La informática jurídica documental, intimidad, el *habeas data* y el estado. 4. La criminalidad concomitante con el desarrollo tecnológico: el hecho punible informático. **II. LOS DELITOS CONTRA LA INTIMIDAD** 1. La intimidad y la informática en la constitución de 1991. 2. La intimidad como bien jurídico tutelado. 3. La intimidad personal y familiar en la jurisprudencia de la corte constitucional: la tutela como vía de protección y defensa. 4. La intimidad o "la vida privada" en el código nacional de policía. 5. La intimidad de las comunicaciones en el código penal de 1980. 6. La intimidad como bien jurídico tutelado en el código penal del 2000. **III. LOS DELITOS CONTRA LOS DATOS PERSONALES Y EL HABEAS DATA.** 1. Cómo surge el término "habeas data" 2. La conceptualización del habeas data. **3.** Tipos delictivos contra los datos personales y el habeas data. BIBLIOGRAFIA

RESUMEN

El presente estudio jurídico, hace un análisis conceptual del derecho fundamental de la intimidad, los datos personales y el *Habeas Data*, que en principio se acuñó en el constitucionalismo del Brasil producto de los trabajos doctrinales y legislativos y luego se extendió al derecho latinoamericano. Colombia lo recogió en el artículo 15, Inciso 1º and 2º de la Constitución de 1991 y recientemente lo reglamentó en forma parcial desde el punto de vista la información o datos financieros en la Ley 1266 de 2008, la cual fue declarada exequible por la Corte Constitucional colombiana en Sentencia C-1101 de 2008. Por su parte, la Ley 1273 de 2009, adicionó en forma parcial el actual Código Penal Colombiano de 2000, al crear un nuevo bien jurídico que protege las *informaciones y los datos personales*, creando nuevos delitos que afectan el llamado *habeas Data* y los datos personales, tales como: la interceptación de datos personales, el uso de software malicioso; la violación de los datos personales; la suplantación de sitios de web para capturar datos personales; entre otros.

ABSTRACT

This law firm makes a conceptual analysis of the fundamental right of the intimacy (or Right to privacy), the personal dates and the *Habeas Data*, which was originally coined in Brazil constitutionalism of the work product doctrine and legislation and then spread to Latin American law. Colombia picked him up in Article 15, Paragraph 1 and 2 of the Constitution of 1991 and recently regulated in part from the standpoint of information or financial data in Law 1266 of 2008, which was declared admissible by the Colombian Constitutional Court in Sentence C-1101-2008. For his part, Law 1273 of 2009, partially added the current Colombian Criminal Code of 2000, creating a new legal right that protects *information and personal data* creating new crimes that affect the so-called *habeas data* and personal data, such as the interception of personal data, the use of malicious software, the violation of personal data spoofing web sites to capture personal information, among others.

(*) Docente Titular de Derecho Público, Facultad de Derecho de la Universidad de Nariño (Colombia) desde 1986 hasta la actualidad. Magister en Criminología de la USTA-UDENAR, 1994. Doctor en Derecho Administrativo en la Universidad de Navarra, 1986 y en Derecho Constitucional de la Universidad de Lleida, España 1999. Autor de obras jurídicas de derecho público y colaborador de la Revista de Informática Jurídica, Dirigida por el Dr. José Cuervo. Mi Correo: lriascos@udenar.edu.co. 2013.

I. LOS DELITOS INFORMATICOS CONTRA BIENES JURIDICOS INTANGIBLES

1. NOTAS PRELIMINARES. A partir de la segunda mitad del presente siglo --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 priori-zarse, 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, tal y como se puede constatar con la simple lectura de los diversos catálogos punibles de los Estados modernos incluidos 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., o bienes jurídicos específicos, como los patrimoniales y socio-económicos [2].

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 multi-tratamiento de la informa-

---

(1) Nos referimos a los Estados de *la Commonwealth (*Inglaterra, Canadá, Australia, Irlanda del Norte, Nueva Zelandia, entre otros) 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". (Oppenheim). En: www.austlii.edu.au

(2) RIASCOS GOMEZ, Libardo O. ***La Constitución de 1991 y la informática jurídica.*** Ed. UNED, Pasto (Col), 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 (art. 15) de los "riesgos" sobrevinientes de la informática contra los derechos fundamentales.

(3) En éste sentido: 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. 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,*** 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.

ción 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 (o "personal computer"-PC- u "ordenadores" [5]), corporativos o empresariales e incluso industriales ("hardware": unidades de procesamiento y periféricas [6]); y sobre todo, por el fácil acceso, tratatratamiento, uso y abuso de programas computacionales o "software", los "ficheros" [7] 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. REGULACION IUSPENALISTA DEL DERECHO DE ACCESO A LA INFORMACION, EL HABEAS DATA Y LA INTIMIDAD.

El proceso de tratamiento informatizado de la información o de los datos de carácter personal, comporta una serie de etapas, fases o ciclos informáticos, tales como recolección, almacenamiento, registro, circulación y transferencia. 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 y libertades 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 España y Colombia (v.gr. arts. 18 y 20.1.d) CE., y arts. 15 y 20 Constitucional). 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 correspon-

---

(4) 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 Acelex".*** Ed. Comunidad Europea, Bruselas, (B), 1997., pág. 20

(5) La traducción del término francés "Ordenateur" al castellano "Ordenador", es el que se ha impuesto en la legislación, doctrina y jurisprudencia españolas, en tanto que el término inglés "computer" ("computador"), es el que se ha aceptado en un amplio sector del mundo.

(6) La Unidad de Procesamiento Central *(Central Processing Unit,* CPU), que es como el "cerebro" del computador, pues allí se desarrolla el principal trabajo electromagnético y mecánico. En términos sencillos, es la parte del computador que hace posible la emisión y recepción o tratamiento propiamente dicho de la información. Esté como las unidades periféricas, o también llamados "soportes informáticos", son aquellas partes que rodean, auxilian, complementan y confirman un procedimiento informático (monitores, teclados, discos, impresoras, etc). A todo esto, se denomina Hardware básico o primario. Vid. Mi trabajo. ***La Constitución de 1991 y***... Ob. ut cit.págs. 128 a 242.

(7) "Fichiers", es la versión francesa de la castellana "Ficheros". En la versión inglesa son "Banks". Una y otra se entiende como un conjunto coherente de datos personales que previo un tratamiento informatizado ("in"), pueden ser accedidos o recuperados ("input" or "output"), por las personas interesadas o terceros, o por los responsables de su vigilancia y control, cuenten o no con autorización para hacerlo. La disyuntiva de la autorización o no marca la licitud o ilicitud en el acceso, uso o conservación.

diente equilibrio ponderado que deviene principalmente de los límites constitucionales y legales de los derechos y libertades fundamentales en éste involucrados.

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) [8]; 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. Reglamentada por el R.D.1332/1994, de 20 de Junio. 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 en Colombia [9].

Toda esta normatividad que concatena, a nuestros efectos, los derechos de la información, el habeas data y la intimidad en los diversos Estados constituye además, el cuerpo legislativo complementario, de interpretación y hermenéutica del derecho punitivo o de "*normatividad extrapenal*" [10], y por tanto, de ineludible observancia.

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".

---

(8) AA.VV. ***Base de datos de la universidad de Montreal (Canadá***). Departamento de Derecho Público. Biblioteca Virtual (Inglés-Francés). Vía Internet (WWW.UMONTREAL.EDU.CA), págs. 1 y ss. AA.VV. Base de datos de la universidad de Australia. Vía Internet. (www.austlii.edu.au), págs. 1 y ss.

(9) Estatuto del derecho a la información: Ley 57 /85, de 5 de Julio, Código Contencioso Administrativo y el Reglamento aprobado por la Junta Directiva de la Asociación Bancaria y de Entidades Financieras de Colombia, de 23 de Marzo 23 de 1995, relativa a la *información económica y financiera* sometida a tratamiento y procedimiento informatizado de carácter privada con competencias sólo de buena gestión y manejo del sistema informático, creado o puesto en funcionamiento por la Central de Información de ASOBANCARIA --CIFIN-- , pero no de sanción. En consecuencia, la Superintendencia Bancaria no tiene funciones de control, gestión, ni mucho menos de sanción sobre los bancos de datos que la CIFIN gestiona, "ni de las personas que lo administran, pues se trata de personas jurídicas diferentes a las vigiladas, a las cuales prestan su servicio para la evaluación del riesgo de su clientela"(CC. Sentencia T-486/1992, de 11 de Agosto. Sentencia T-414/1992,de 16de Junio). Textos completos en WWW.RDH.GOV.CO . 1998.

(10) 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. Ed. Aranzadi, Pamplona (Navarra), 1996. pág. 309 y ss.

Los Códigos Penal español y canadiense hacen referencia específica a la intimidad como bien jurídico protegido, 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 tecno lógicos (art.184.3); 4. Interceptación judicial de datos en circunstancias excepcionales (art. 184.4); 5. Interceptación de datos o información a través de dispositivos electromagnéticos, 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* [11], 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, Tít. X, del C.P. del 95 (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 nueva LORTAD y los delitos del artículo 197.2, pues a su juicio, la nueva 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 consecuencia, 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

---

(11) MORALES PRATS, Fermín. ***La tutela penal de la intimidad: privacy e informática***. Ed. Barcelona (Esp.), 1984. págs. 60 a 81. Ibídem. ***Delitos contra la intimidad...***.Ob. cit. pág. 312 y ss. Ibídem. ***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. Sobre el tratamiento de datos (LORTAD y Dec.1332/94, Directiva 95/46/CE).

LORTAD en el ciclo operativo del banco de datos". *Arroyo Zapatero* [12], 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 [13], o más aún, cuando infracciones y sanciones administrativas [14] por su contenido son verdaderos delitos y penas [15], correspondientemente suavizados por la mano mágica de la naturaleza iusadministrativa.

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 y telemáticos.

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

---

(12) 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.

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

(14) La protección a la "privacidad" (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. 43 y ss de la nueva LORTAD, como "infracciones leves, graves y muy graves", y sostiene que ésta "parece 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.), 1 ed., 1987, y 2 ed. 1994, p.179.

(15) 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 43 y ss., de la nueva 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.

prevé una y otra clasificación [16] .

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).

En Colombia, como precisaremos *ut infra*, el derogado Código Penal de 1980, no tenía 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 postindustrial 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 el artículo 15 de la Constitución Colombiana de 1991, a pesar de que el derogado Código Penal 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 *habeas Data e Intimidad.*

En efecto, el Titulo II de la Constitución, relativo a "los derechos, las garantías y los deberes", Cap. I. "De los Derechos Fundamentales", en el artículo 15 sobre el "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: A *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 autolímite 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 (T-022-92).

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 límitados por la propia constitución y los demás derechos.

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*

---

(16) VALLE MUÑIZ, **José Manuel** y MORALES PRATS, **Fermín**., Ob.ut supra cit. Se refieren a los delitos contra el patrimonio económico y contra el orden socioeconómico -- Tít.XIII-- (Delitos contra los datos) y los delitos contra la intimidad --Tit. X--, los relativos al ejercicio de los derechos fundamentales y libertades públicas --Tit. XXI, Cap. V-- y los previstos en leyes penales especiales. v.gr. La propiedad intelectual (Delitos de los 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 límitados por la propia constitución y los demás derechos.

Sin embargo, el Código Penal de 1980, bajo el concepto genérico de libertades públicas subsumía a la intimidad como bien jurídico protegible de cualquier conducta humana que utilice medios electromagnéticos, computacionales o telemáticos en el Título X, Cap. V., 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 derogada del Decreto Extraordinario 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 (art. 21 Constitucional) u "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 del C.P.), al estar incorporados en el bien jurídico tutelado de "la Integridad Moral".

El hecho punible en Colombia se divide en delitos y contravenciones (art. 12 del C.P.), y éstas a su vez se dividen en ordinarias y especiales. El Código Nacional de Policía (Decretos 1355-2055 de 1970 y 522 de 1971, modificados parcialmente por la varias Leyes, aún están vigentes), protege la Intimidad personal y familiar de las personas al erigir como contravenciones especiales una serie de conductas que afectan la información y los datos personales, así como la inviolabilidad de habitación y domicilio. En efecto, las contravenciones especiales, entre las que están (i) la averiguación de la vida íntima o privada (artículo 46); (ii) divulgar la vida privada o íntima (artículo 47); (iii) indiscreción de la vida privada (artículo 48); y (iv) la presencia injustificada en domicilio ajeno (artículo 56) que son las más graves entre las contravenciones, son investigadas y juzgadas a través de procedimientos policivos por las autoridades administrativas municipales (Alcaldes e Inspectores de Policía) y departamentales (Gobernadores y autoridades delegadas en lo policivo), con funciones cuasi jurisdiccionales[17].

Estas contravenciones, según el Código de Policía, "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.

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, los datos personales y el habeas data). La intimidad como bien jurídico protegido cuando hace referencia a los "*Delitos contra la libertad individual y otras garantías", y la "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) *Violación ilícita de comunicaciones o correspondencia*

---

(17) RIASCOS G. Libardo. ***La jurisdicción civil de policía.*** Tesis para optar el título de abogado, Universidad de Nariño, Facultad 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.

de carácter oficial (art.196); y, 5) *Utilización ilícita de equipos transmisores o receptores* (art.197).

La Ley 1273 de 2009 que reformó parcialmente el Código Penal del 2000, creó el Titulo VII Bis, relativo a los delitos contra "la información y los datos" personales en dos capítulos: El primero, relacionado a "los confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos" y dentro de éste, los siguientes delitos (artículos 269 A a 269 G): (i) Acceso abusivo a un sistema informático; (ii) Obstaculización ilegítima de sistema informático o red de comunicación; (iii) Interceptación de datos informáticos; (iv) Daño Informático; (v) Uso de software malicioso; (vi) violación de datos personales; y, (vii) suplantación de sitios web para capturar datos personales. Además, se regula ocho causales de agravación punitiva aplicables a las anteriores conductas delictivas en el artículo 269 H, aunque algunas de ellas ya se encuentran inmersas en algunos delitos v.gr. el delito de violación de los datos personales, ya incorpora en el tipo, la causal de "provecho propio o de un tercero" que es la causal de agravación 5º.

En el Capítulo II, relativo a los "atentados informáticos y otras infracciones", previstos en los artículos 269 I y 269 J, están los delitos de "hurto por medios informáticos y semejantes" (se entiende por tales, los electrónicos y telemáticos); y el delito de "transferencia no consentida de activos.

3. LA INFORMATICA [18] JURIDICA DOCUMENTAL, INTIMIDAD, El *HABEAS DATA* Y EL ESTADO.

Algunos Estados del mundo han constitucionalizado prematura o tardíamente "el uso", "la aplicación" o "la utilización de la informática" a los efectos limitar o restringirla con claros efectos proteccionistas o garantístas de derechos fundamentales, como en el caso de España, Colombia y Portugal, respectivamente. En efecto, se constitucionaliza para "garantizar" el derecho a la intimidad personal y familiar de los ciudadanos, la imagen, el honor y A el pleno ejercicio de sus derechos", según la Constitución Española de 1978 (art. 18.4), o además de ello, para aplicarlo en el ejercer el derecho de *habeas data* (acceso, actualización y rectificación de la información) dentro del proceso de tratamiento electromagnético público y/o privado, que tiene toda persona, según La Constitución colombiana de 1991 (art. 15); o más aún, como derecho fundamental aplicable todo "utilización de la informática" y para prohibirla expresamente en el tratamiento de datos de carácter personal sobre aspectos filosóficos, de filiación política o sindical, de fe religiosa o vida privada "salvo cuando se trate de procesamiento de datos de carácter estadístico no

---

(18) La STC 254/1993, Jul.20 y STC /1994, Mayo 9 de 1994. Sala 1. Se reconoce y destaca la importancia actual. Reconocimiento que ha sido reiterado por posteriores pronunciamientos del Tribunal Constitucional. STC Mayo 9 de 1994. TC1 y STC Enero 13 de 1998, TC1, FJ.4, en el cual se sostuvo: A Por su parte, la STC 254/1993, declaró con relación al art.18.4 CE, que dicho precepto incorpora una garantía constitucional para responder a una nueva forma de amenaza concreta contra la dignidad y a los derechos de la persona. Además de un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, es también, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos (FJ.6). La garantía de la intimidad, *latu sensu*, adopta hoy un entendimiento positivo que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada libertad informática es así derecho a controlar el uso de los mismos datos insertos en un programa informático *(habeas data*) y comprende entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquél que justificó su obtención (FJ7).

individualmente identificadas", como en la Constitución Portuguesa de Abril 2 de 1976 [19]. A este fenómeno constitucionalizador mundial sobrevino una creciente reglamentación legal para completar el cuadro garantísta de los derechos fundamentales, tal como lo hizo España con cierta demora y excesiva buena expectativa frente al avance del fenómeno tecnológico de la información y la comunicación al expedir la LORTAD y la nueva LORTAD, L.O. 15 de 1999 y su cascada de decretos reglamentarios[20], pues ya otros Estados del entorno europeo existían sus leyes con excesos o defectos, con falta de incardinación entre lo prematuro y lo desfazado del fenómeno tecnológico y las normas jurídicas por expedir; en fin, entre las experiencias para recoger o desechar al respecto. v.gr. Dentro de las normas prematuras, pioneras pero no sin defectos mínimos a la época están: La "*Data Lag*" Sueca de 11 de Mayo de 1973; Las alemanas : a) *Land de Hesse* en Alemania, promulgada el 7 de Octubre de 1970; y, b) La Ley Federal de Protección de Datos de 27 de Enero de 1977, reeditada en la nueva Ley de 20 de diciembre de 1990; y más recientemente, La Ley francesa "relativa a la informática y a los ficheros y las libertades" de Enero 6 de 1978 y la Suiza de 16 de Marzo de 1981; entre muchas otras dentro y fuera del contexto europeo, como las citadas anteriormente de Canadá y Australia.

El art. 15 de la Constitucional, en su parte inicial expresa: "*Todas las personas...Tienen 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.",* y más adelante complementa al indicar cuál es el procedimiento de recolección, tratamiento y circulación de datos o informaciones. Este fenómeno jurídico en la doctrina y legislación universal y más en la latinoamericana, se ha conocido como *habeas data*, que algunos estados como los mencionados han elevado a rango constitucional en tanto que otros como España lo han reglamentado en la ley. Sin embargo, unos y otros reconocen su importancia capital en el juego pleno del respeto, protección y límites de los derechos fundamentales, además de considerar que las nuevas tecnologías de la información y comunicación (informática y/o telemática) están íntimamente ligados con éste fenómeno; y por eso, el carácter expresamente, y en no pocas veces, exageradamente proteccionista de los estados ante la irrupción agresiva de aquéllas, como no había sucedido desde las revoluciones postindustriales en el mundo.

En efecto, hoy más que nunca, se impone la pregunta: ¿Por qué la informática, revolucionó muchas facetas de la vida humana, en particular la visión del derecho penal y la actuación del Estado frente a éste?.

Las razones son variopintas, algunas de ellas las ha contestado el profesor *Hernández Gil*, al analizar el derecho, la informática y la ciencia y al encontrar que el derecho va a experi-

---

(19) AA. VV. ***Constituçiâo Novo Texto.*** Ed Coimbra. Ediçâo organizada J.J. Gomes Canotilho o Vital Moreira, Portugal, 1982. pág. 29

(20) La doctrina española era consciente de esa demora porque el entorno normativo europeo, así como la normativa de influencia en la UE (Unión Europea) establecía un status, unas directrices sobre regulación y protección en estas materias. V.gr., el Convenio de Europa de 1981, el cual, más tarde fuera retomada en la Directiva 95/46/CE, Parlamento Europeo y del Consejo, de 24 de Octubre de 1995, sobre la "protección de personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos". El profesor Davara, analiza el hecho de la demorada aparición de la LORTAD, explica que la demora no fue del todo buena, pues no se entiende todavía como persisten en ésta ley, "las rígidas excepciones que se establece en ´favor´ de los ficheros de titularidad pública y el ambiguo régimen y regulación del órgano de control --llamado Agencia de Control de Datos-- que crea la propia ley". Vid. DAVARA R. Miguel. ***Manual de Derecho Informático.*** Ed. Aranzadi, Pamplona (Esp), 1997. pág. 70. En igual sentido: DEL PESO NAVARRO, Emilio. ***La seguridad de la información.*** En: Actualidad Informática Aranzadi. A.I.A. Núm. 26 de Enero, Ed. Aranzadi, Elcano (Navarra.), 1998, pág. 1 y ss.

mentar un cambio en sí mismo, tras observar las nuevas realidades tecnológicas y el modo diferente en el que va a ser elaborado, tratado o conocido por éstas. El Tribunal Constitucional Español (STCS: 254/1993, Mayo 9/1994, Enero 1/1998); por su parte, ha evidenciado la importancia tras fijar el contenido esencial del derecho a la intimidad y de otros derechos fundamentales previstos en la CE, así como los límites constitucionales de existentes entre éstos y las posibles agresiones que pueden sobrevenir con las nuevas tecnologías de la información y comunicación (TIC): informática y/o telemática, tal y como concretaremos más adelante. Este repertorio de impactos tecnológicos no solo temporales sino de contenido han sido continuos, constantes y cada vez más sofisticados (v.gr. La Multimedia), estructura una nueva forma de estudiar, analizar y crear el derecho, y en particular en el ámbito penal. Así, el poder "subversivo" de la informática y telemática avanza acarreando consigo esa dicotómica consideración: por un lado, la de servir de vehículo actual, idóneo y visionario en la potenciación del tratamiento, procesamiento, divulgación o consulta de la información documentaria generada por el derecho, en general; y por otro, la de considerarse como una gran amenaza de carácter tecnológica en manos de quienes ilícitamente acceden, utilizan, usan, conservan o divulgan información o datos públicos o privados en contra de derechos y libertades públicas o bienes jurídicos.

En efecto, con el advenimiento de las tecnologías de la información y comunicación (TIC), los juristas y el Estado mismo, comenzaron a replantearse la mejor forma de organizar el producto intelectivo de su actividad diaria (v.gr. Labor en oficinas particulares y públicas; el cúmulo de providencias judiciales, en el ámbito judicial; normas jurídicas, en el ámbito legislativo; normas administrativas, procedimientos gubernativos, estatutos; en el ámbito administrativos, etc.), cuando menos, en la parte más relevante de la información jurídica; es decir, en la que se crea, modifica, suspende o extingue derechos y/o libertades públicas, o que afectan directa o indirectamente aquéllas y persiguen su tutela y protección estatal. Toda esta Información años atrás se había mantenido en grandes soportes impresos o documentos escritos, en extensas bibliotecas generales y especializadas. Su incorporación, organización, conservación; y sobre todo consulta resultaba lenta, muchas veces engorrosa y de alta dosis de paciencia.

Como consecuencia, se buscó la mejor forma de ingresar, ordenar, clasificar y recuperarse el cúmulo de datos en forma automatizada (informática y/o telemática), a través del documento electromagnética, a fin de potenciar y eliminar la mayoría de obstáculos que representaba el documento impreso o escrito, y en realidad de verdad se consiguió en un alto porcentaje, no sin sacrificio, limitación o surgimiento de nuevas como variadas amenazas, principalmente a los derechos fundamentales o de expectativas *per se* devenidas de la tecnología, tal como analizó en el capítulo anterior, al comentar la informática jurídica documental, como parte de la informática jurídica.

Antes de la denominada época "postindustrial", no se podía escoger entre el archivo y tratamiento documental de la información por mecanismos manuales o tecnológicos. A partir de ésta época en mayor proporción el tratamiento se hace electromagnéticamente con aparatos y equipos informáticos y telemáticos, generando así una nueva cultura del tratamiento de la información producida por el derecho, pero a la par nuevos y variados riesgos, atentados y agresiones ilícitas públicas y privadas devenidos de esa tecnología. Los Estados, por su parte, como se ha dicho, han tomado una doble postura: una, preventiva, civilista y administrativa (*o de prima ratio)*; y otra, represiva (o *de ultima ratio)* previa la catalogación de tipos penales generales o específicos que tipifican "delitos informáticos" o hechos punibles en los que el fenómeno informático y telemático está presente como medio u objeto material de la comisión y/o ejecución del *iter criminis,* y en ambos casos, con excesiva "punibilidad", no totalmente justificada desde el punto de vista de una política criminológica de Estado frente a las nuevas tecnologías de la información y comunicación, como sucede en

España [21], Australia [22], al crear tipos penales que atenta contra el derecho a la intimidad de las personas u otros bienes jurídicos como el patrimonio económico, la propiedad intelectual, etc. Igualmente, en el caso colombiano al agravar los tipos penales en los que se halle vinculada la tecnología informática o telemática, así se atente contra derechos fundamentales (la intimidad o el habeas data, honra, etc) o bienes jurídicos (patrimonio económico, fe pública, etc.). Más adelante puntualizaremos sobre el tema.

4. LA CRIMINALIDAD CONCOMITANTE CON EL DESARROLLO TECNOLOGICO: EL HECHO PUNIBLE INFORMATICO.

4.1. En España, la legislación y doctrina mayoritaria no aceptan la existencia del delito informático. Por excepción, se acepta, teoriza y más aún , se clasifica.

4.1.1. Primera Postura: No existe el delito informático.

En Europa, a excepción de España, algunos Estados han regulado en sus códigos penales o leyes especiales, el denominado "delito informático", como veremos más adelante. En España, un gran sector de la doctrina iuspenalista, consideran incluso inadecuada hablar de la existencia como del nomen iuris de "delito informático", en el actual Código Penal de 1995, o en Leyes penales especiales o las extrapenales, como la LORTAD (Ley Orgánica No. 5, sobre la regulación del tratamiento automatizado de los datos de carácter personal de Octubre 29 de 1992), aunque esta última es de naturaleza iusadministrativa, la doctrina reconoce que esconde figuras delictivas.

Davara Rodríguez [23] , con base en el principio penal universal de *nullum crimen, nulla poena, sine lege*, estima que no habiendo ley que tipifique una conducta delictiva relacionada con la informática como bien jurídico protegido, ni que se haya determinado una pena para tales conductas, se puede concluir que no existe delito ni pena por las acciones tentadas o consumadas, por más dolosas que éstas sean.

Así mismo, deshecha el principio de la analogía de la teoría general del delito para aplicarlo a los llamados delitos informáticos, pues considera, el autor citado, que éste sólo será aplicable cuando beneficie a un "encausado", pero no para crear nuevos delitos, como se pretende por quienes quieren ver delitos informáticos tras haber incorporado el Código Penal del 95, figuras delictivas que atenta bienes jurídicos específicos como la Intimidad, el Honor, el Patrimonio y el orden socio-económico y que utilizan medios comisivos informáticos y telemáticos.

---

(21) En efecto, así se prevé como puntualizaremos más adelante (punto 5) y aunque la legislación y doctrina no reconoce la existencia tabulada en el C.P.de 1995, ni en ninguna otra ley especial de los llamados "delitos informáticos", pero sí la existencia de ilícitos penales en donde se utilizan medios comisivos informáticos o telemáticos o incluso en aquellos delitos que de alguna forma interviene un "elemento informático" y que atenta contra un bien jurídico definido como la Intimidad (Tit. X), el Honor (Tít. XI), o el "Patrimonio y el orden socio-económico (Tit.XIII); entre otros. Una visión de precisa crítica al respecto se hace en el trabajo realizado sobre el título X del C.P.del 95, cuando se sostiene que "la gravedad de las penas que se establecen para casi todos los supuestos puede llevar en algún caso a violar el ´principio de culpabilidad´, pues a la infracción cometida se fija una pena desproporcionada". SERRANO GOMEZ, Alfonso. ***Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio.*** En: Derecho Penal- Parte Especial. Ed. Dykinson, 2a, ed., Colaboración de Alfonso Serrano Mailló, Madrid, 1997. págs. 225 a 238.

(22) En Australia, sí se tipifica claramente los delitos informáticos en la "Crimes Act 1914", como "*Computer Crime" En el "Act*", en las partes VIA (Arts. 76A a 76E y parte VIIB (Art. 85E,F), sobre delitos contra los datos o "informaciones personales" a través de medios electromagnéticos, telemáticos y computacionales

(23) DAVARA R., Ob. ut supra cit., pág.285-304. La posición de Davara es compartida por varios iuspenalistas como Valle Muñiz, Bueno Arús, Pérez Vallejo, Bustos Ramírez, Bajo Martínez; entre muchos otros.

Sin embargo, el autor citado reconoce el impacto actual de las tecnologías de la información y la comunicación en la comisión de delitos, así como la necesidad de utilizar la nomenclatura de "delitos informáticos", para abarcar ese gran sector de la nueva criminalidad en los que se emplea a la informática o la teletransmisión de datos o informaciones como medios para cometer un delito, o para "otras referencias a la informática y /o a la telemática, que figuran en el nuevo Código Penal" Español de 1995, *por conveniencia, para referirnos a determinadas acciones y omisiones dolosas o imprudentes, penadas por la ley, en las que ha tenido algún tipo de relación en su comisión, directa o indirecta, un bien o servicio informático* [24] .

Con aquéllas finalidades, *Davara* [25] define el delito informático como *la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software*. En esta definición el autor sin quererlo aplica el concepto analógico del delito en términos generales previsto en la legislación española vigente y el vertido en las recomendaciones de la Organización para la Cooperación Económica y el Desarrollo Europeo (OCDE) [26]. Así mismo, incorpora no convenientemente en el mismo concepto, por un lado, todas aquellas acciones punitivas cuya comisión se realiza con medios o equipos informáticos, electromagnéticos, audio-visuales o de teletransmisión de datos; y por otra, las acciones punitivas que atenta derechos fundamentales, como la intimidad, la honra, etc., o bienes jurídicos tutelados por la ley, en los que se utiliza algún "elemento informático", bien sea logicial o de programas computacionales (software) o equipos físicos centrales o periféricos computacionales (hardware).

4.1.2. Segunda Postura: Posición ecléctica.

Sin embargo, *Pérez Vallejo* [27], recuerda que si bien no podemos hablar de delitos informáticos en la actualidad, la protección jurídica de la propiedad intelectual goza de raigambre en la legislación penal española desde el catálogo punitivo fundamental de 1848, aunque sostiene también, que por la aparición de nuevos los fenómenos tecnológicas ésta ha tenido que cambiar su regulación en la L.O. 10/95, para bien aunque parcialmente, puesto que se reprimen aquellas defraudaciones que centran su actividad principal en el acceso y manipulación de datos que se encuentran en soportes informáticos, o de programas de computador utilizados en su procesamiento.

4.1.3. Tercera Postura: El delito informático existe doctrinalmente.

Doctrinalmente se acepta la existencia del delito informático antes como después de la vigencia del Código Penal Español de 1995, tras analizar los contenidos normativos de otras latitudes como el ordenamiento jurídico-penal español.

---

(24) Ibídem pág. 304

(25) Ibídem pág. 288.

(26) La OCDE, creada en 1948, como organización de cooperación preferentemente económica entre Estados Europeos que hoy forman la UE (Unión Europea), EE.UU y Canadá (1960), Japón (1964), Finlandia (1969), Australia (1971) y Nueva Zelandia (1973). Delito informático, según la OCDE es: "cualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento automatizado de datos y/o a la transmisión de datos". Davara critica válidamente esta definición cuando sostiene que ésta no es muy técnica al apartarse del concepto mismo del delito y mencionar genéricamente a toda "conducta ilegal", cuando se puede tratar perfectamente de una acto tipificado en la legislación penal "y el ordenador haber resultado accesorio por completo en la realización del mismo".

(27) PEREZ VALLEJO, Ana. ***La informática y el derecho penal***. En: Actualidad Informática Aranzadi. A. I.A. Núm. 19 de Abril, Ed. Aranzadi, Elcano (Navarra.), 1996., pág.8 a 12.

En efecto, el profesor *Romeo Casabona* [28], estudia la posibilidad de estructurar un nuevo bien jurídico denominado de la "información sobre la información", como un bien que comporta por sí sólo un valor (económico, de empresa o ideal), relevante y digno de tutela jurídico-penal. Este valor será tan importante como para que la conducta humana sea calificada jurídicamente y pueda imponérsele una sanción correspondiente. Con base en esta estructuración, el autor citado siguiendo las clasificaciones de *Lamper y de Sieber* -- como lo afirma *Pérez Vallejo* [29]--, clasifica a los delitos informáticos en cuatros grupos o categorías. Clasificaciones que sirven a la citada autora, a *Gutiérrez Francés* [30] y *Buenos Arus* [31], para hacer su estudio sobre el delito informático en la legislación española antes de la vigencia del Código Penal de 1995 y con base en los anteproyectos y proyecto de Código Penal de 1992, pero a diferencia de todos ellos, el profesor Romeo Casabona, considera la información como valor no estrictamente ni sólo económico, sino que conlleve un valor relevante y digno de tutela jurídico penal.

Hoy por hoy, este derecho fundamental a la información o "derecho a ser informado", tiene su asidero en el art. 20.1 d), de la CE., y consiste en que toda persona tiene derecho no sólo para comunicar sino a "recibir" de las autoridades del Estado o las personas jurídicas públicas o privadas información concreta, oportuna y veraz dentro de los límites de la Constitución y el Ordenamiento Jurídico. No es simplemente la "otra cara" del derecho a comunicar la información, ni a emitir libremente sus ideas y opiniones, ya de palabra, ya por escrito, valiéndose de Prensa e Imprenta o de otro medio, sin sujeción a censura previa, como estaba previsto en las Constituciones Históricas Españolas, sino un derecho autónomo, complejo, dinámico, público y democrático según lo sostiene *Villaverde Menéndez* [32], por el cual, el Estado debe proteger a quien ocupa la posición de sujeto pasivo de la libre discusión de las ideas (opiniones e información) y a quien participa en él activamente como un emisor de las mismas; además, al receptor de esas ideas del propio emisor, el cual puede engañar o manipular a los receptores. No debe olvidarse que hoy en día por la universalización de los medios de comunicación social, el cúmulo de información que se emite y recibe es cada día mayor y los ciudadanos están expuesto en ese flujo constante de ida y venida de toda clase de información relevante y no únicamente aquella llamada con "valor económico de empresa". Por su parte el acceso a la información como derecho fundamental de toda persona, encuentra su fundamento constitucional en el art. 18 CE., cuando se reconoce genéricamente la limitación de la informática con relación a los derechos personalísimos de la intimidad, la propia imagen, el honor y el *pleno ejercicio de los derechos* fundamentales (STCS 254/1993 y Mayo 9/1994). Este derecho de acceso como el de actualización, rectificación y cancelación de la información se halla reglamentado en la LORTAD y Dec.1332/94, arts.12 y ss., principalmente.

Por su parte*, Carbonell y González,* [33] al estudiar el art. 197.2 del Código Penal Español del 95, lo intitula: "*Los delitos informáticos"*, para seguidamente expresar que éste numeral

---

(28) ROMEO CASABONA, C.M., ***Poder informático y seguridad jurídica.*** En: Cuadernos de Derecho Judicial. Escuela Judicial. Consejo General del Poder Judicial. C.G.P.J, "Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías", Madrid, 1993. Cit. Ob. Arus, pág. 2.

(29) PEREZ Vallejo, A. Ob cit., pág. 9.

(30) GUTIERREZ F., Mariluz. ***Notas sobre la delincuencia informática: atentados contra la "información" como valor económico de empresa***. En: Estudios de Derecho Penal Económico. Editores Luis A. Zapatero y Klaus Tiedemann. Ed. Univ. De Castilla-la Mancha, Tarancón (Cuenca), 1994. Pág. 183.

(31) ARUS B. F. Ob. cit ut supra. pág. 2 a 6.

(32) VILLAVERDE MENENDEZ, Ignacio. ***Los Derechos del Público.*** Ed. Temis, Madrid, 1995, pág. 15

(33) CARBONELL M. J.C. y GONZALEZ C.J.L., ***"Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio."*** En: Comentarios al Código Penal de 1995. Vol. I. Ed. Tirant lo blanch. Valencia, 1996, pág. 999

contiene a éstos delitos, “aunque en puridad --dice-- se deberían llamar delitos contra la intimidad de las personas mediante el uso de la informática y de las comunicaciones”. Sin embargo, creemos los autores observan parcialmente el carácter por parte de la informática, que en éste caso es a la intimidad, pero no observan el de riesgo o inminencia atentatoria de un derecho fundamental o bien jurídico protegido del fenómeno informático en forma holística, pues el misma art. 18 CE, sostiene el complejo asunto de los autolímites al ejercicio y potestad de los derechos fundamentales y en ellos se menciona no sólo a la intimidad, la propia imagen sino al honor y *el pleno ejercicio de sus derechos*[34], con lo cual por defecto en el nomen iuris, podríamos entender por delitos informáticos, solamente a los delitos que atenta contra la intimidad. Súmese a ello, que en el C.P. del 95, existen otros derechos y bienes jurídicos llamados patrimoniales en los que la informática constituye ese potencial de riesgo e inminencia atentatoria que comentamos y que quedarían por fuera de la previsión planteada por los citados autores. En estas circunstancias el delito informático sólo contra la intimidad queda autodesvirtuado, al menos en el *nomen iuris,* en los términos de los autores citados.

Por contra, al derecho a la intimidad que subsume el de la propia imagen, el derecho al “honor”, no ha sido objeto de regulación jurídico penal en cuanto a los riesgos o atentados que supone la informática o telemática, en los términos del art. 18 de la CE. Sin embargo, la LORTAD, sí prevé infracciones y sanciones administrativas con el objeto de tutelar el honor contra atentados de las nuevas tecnologías de la información y comunicación. En la exposición de motivos de la ley, en el apartado séptimo (7), se precisa que *la Ley no consagra nuevos tipos delictivos, ni define supuestos de responsabilidad penal para la eventualidad de su incumplimiento*, cuando en los arts. 42 y 43 enuncian las infracciones graves, muy graves y leves.

4.1.4. Cuarta Postura: Clasificación del delito informático, en especial los que vulneran el derecho a la intimidad y la información (datos personales)

4.1.4.1. Clasificaciones guiadas por del derecho alemán. El bien jurídico tutelado: “La información”.

Antes de la vigencia del Código Penal de 1995, *Gutiérrez Francés* [35] *,* clasifica al delito informático, en tres grandes categorías, previamente a considerar la información con un valor estrictamente económico de empresa: “lo que tradicionalmente hubiera tenido una mera acumulación de datos, hoy, a causa del impacto de la revolución informática, se ha transformado en un valor, un interés social valioso, con frecuencia cualitativamente distinto, dotado de autonomía y objeto del tráfico”. Sin embargo esa escisión tan cortante de la autora en la realidad no se presenta, valga el ejemplo de la conducta de los *hackers* (fusiladores o intrusos en los datos) sobre cualquier tipo de información. Esta conducta la realizan personas de cualquier edad, verdaderos adictos de la intromisión por placer o por desconocimiento o simple negligencia. Conducta diferente a la realizada por los *crackers* (rupturadores de datos), adictos delirantes que van sobre cualquier tipo de información con el objetivo de dañarla, inutilizarla total o parcialmente con diferentes métodos. Hackers y crackers van a por cualquier tipo de información o datos y no necesariamente los que denotan un “valor económico”. Esto es lo que revela Ley Austriaca de 1987 de 22 de diciembre al tipificar el delito informático de “Destrucción de datos” (126 a ostStGB) en el numeral 2, sostiene: *Se entiende por datos tanto los personales como los no personales y los programas*.

---

(34) En concordancia con el art. 8 del Convenio Europeo de 1981 y los considerandos 2, 4,7, 9 y 10 de la Directiva 95/46/CE. STCS 254/1993 y de Mayo 9 de 1994.

(35) GUTIERREZ F., M. Ob. cit. pág. 184 a 208.

Las tres categorías de *Gutiérrez F*., son: a) El espionaje informático industrial o comercial; b) Las conductas de daños o sabotaje informático que incluyen: la destrucción, modificación o inutilización de archivos y ficheros informatizados con valor económico de empresa; y, c) Las conductas de mero intrusismo, también conocidas por el término anglosajón *hacking.* Advierte, que las fronteras de estas divisiones no son categóricas, así como también que la dinámica comisiva de estos ilícitos pueden propiciar situaciones concursales. v.gr. Un comportamiento de espionaje empresarial puede ir acompañado de una modificación o destrucción de datos, subsumible en la categoría de sabotaje informático.

Posteriormente y en vigencia del C.P.del 95, *Pérez Vallejo* [36]*,* siguiendo las clasificaciones de *Romeo Casabona*, agrupa a los delitos informáticos en cuatro bloques, a saber: a) Alteración de datos (Fraude informático), b) Destrucción de datos (sabotaje informático), c) Obtención y utilización ilícita de datos (espionaje informático o piratería de programas); y , d) Agresiones en el hardware (sustracción de servicios o hurto de tiempo). El término datos o información en la legislación alemana como comunitaria europea, son sinónimos.

Con esta presentación, la autora citada en vigencia del Código Penal del 95, estudia los delitos en los que tiene relevancia la informática para clasificarlos así: a) Delitos de carácter no patrimonial; b) Delitos contra el patrimonio; c) Delitos contra la propiedad intelectual; d) "Otras figuras delictivas", y dentro de la cual involucra; entre otras, al "fraude informático", trayendo a colación la Sentencia de 30 de Noviembre de 1988 de la Audiencia Territorial de Granada, refrendada por el Tribunal Supremo de 19 de Abril de 1991, sobre la interpretación flexible y teleológica de los tipos penales para dar solución a un caso en el que se utilizó un documento mercantil para cometer un delito de falsedad. El documento, objeto de la controversia judicial, no era impreso (no tradicional) --teniendo en cuenta la nueva definición del art. 26 del C.P., del 95-- lo aplicó a un "documento de la (sic) cinta o disco magnético acumulador o estabilizador de datos informatizados".

En el primer grupo: "Delitos de carácter no patrimonial", se ubican los delitos previstos en el Título X, del Código Penal Español, contra la "Intimidad, el derecho a la propia imagen y la inviolabilidad de domicilio", en particular el Cap. I, "Del Descubrimiento y revelación de secretos, entra en una referencia directa a la informática" el art. 197.2. No hace referencia a los delitos contra el honor, a pesar de citar el art. 18 CE., y ser éste otro de los importantes derechos de la personalidad considerado derecho "no patrimonial".

En el segundo grupo: "Delitos contra el patrimonio", se relacionan los "Delitos contra el Patrimonio y contra el orden socio-económico", en particular el Cap.II, sobre "los robos", el robo con fuerza y mediante "uso de llaves falsas" (art. 238.4), es decir, las que enuncia el art.239 y resuelve de paso la controversia que se había presentado con el uso de tarjetas electromagnéticas, pues en la parte *in fine*, considera como llaves falsas "las tarjetas, magnéticas o perforadas". En el Cap. VI, "De las defraudaciones", Sec.I., art. 248.2, contempla la "Estafa informática". En el Cap. IX, "De los daños", el art. 264.2, erige como delito el que "por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos". Se establece así el delito contra el equipo computacional físico o los sistemas y programas lógicos (hardware y software).

En el tercer grupo: *Delitos contra la propiedad Intelectual*, relaciona el Cap. IX: *Delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores* (Tít. XIII, "Delitos contra el patrimonio y contra el orden económico-social" C.P. del 95). En la Sección 1,

---

(36) PEREZ V. A. Ob cit., pág. 9 y ss.

de los delitos contra la propiedad intelectual tipifica algunas conductas en atención a la incidencia actual de las nuevas tecnologías de la información y la comunicación ocasionadas en la obras de creación o intelectuales.

Sobre éste punto es destacar que el C.P., vigente nada nuevo destacable introduce a lo preceptuado en el anterior Código Penal Español., en los arts. 534 bis a) a 534 ter.

4.1.4.2. Clasificaciones del delito informático en donde dos de los bienes jurídicos a proteger más importante son: la *Intimidad* y los datos personales

Sin embargo, es de destacar en el derecho penal español la cuidadosa como compleja redacción de normas que tipifican delitos contra la intimidad y la propia imagen (no así el honor), como derechos fundamentales altamente protegidos en los art. 18.4, 20.1.d) y 105 CE, contra las injerencias de la informática.

El iuspenalista español *Morales Prats* [37], quien se ha preocupado desde su tesis doctoral en 1983, por el estudio del derecho a la intimidad, la informática y el derecho penal, hace un detallado estudio actual y retrospectivo de éste complejo derecho fundamental a la luz de las tecnologías de la información y la comunicación.

En efecto, el autor analiza el Título X, *De los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad de domicilio* (arts. 197 a 204) del C.P., del 95, y considera que la *privacy,* "libertad informática (faceta o perfil informático de la intimidad)", en el art. 197.2, tipifica un elenco de conductas que comportan "abusos informáticos", aunque no en forma completa, pero sí más coherente en la descripción de conductas típicas codificadas y en forma cerrada. No es completa, porque el art. 197.1, recoge las conductas de interceptación, grabación o reproducción electrónica ilícita de comunicaciones informáticas (mensajes de correo electrónico). Igual la captación subrepticia de mensajes de correspondencia electrónica y el apoderamiento físico subrepticio, con la intención de descubrir la intimidad ajena de mensajes de correspondencia informática ya impresos fuera del sistema.

Es coherente, porque finalmente el art.197.2, en su redacción es sustancialmente mejor que la presentada en el proyecto de Código Penal de 1992 (art.198.2) y del proyecto de C.P. de 1994 (art.188.2), textos en los que se tipificaba únicamente el apoderamiento no autorizado de datos personales.

El mentado artículo es una norma cerrada, pues antes que la técnica de tipificación de conductas de ley penal en blanco se escogió la de la codificación y describir las conductas delictivas en forma cerrada para incriminar los delitos contra el *habeas data* o *libertad informática*. Técnica que suscita problemas a la hora de esclarecer las conductas y evidente incorrección en la definición técnica de las conductas típicas, pues para ello hay que recurrir a la LORTAD y otras normas extrapenales que informan las conductas penales previstas en el art. 197.2., como el Convenio de 28 de Enero de 1981 del Consejo de Europa y la Directiva 95/45/CE, del Parlamento y el Consejo de Europa, que completa y amplia la protección del Convenio sobre las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Las conductas típicas previstas en el art. 197.2. CP. del 95, --dice el citado autor- son: a) En el inciso primero, quedan tipificadas las acciones de apoderamiento, utilización o modificación

---

(37) MORALES PRATS, F. Ob. ut supra cit., págs. 299 a 322.

de datos reservados de carácter personal, que se hallen automatizados de forma electrónica o que obren en cualquier otro tipo de archivo o registro público o privado. Estas acciones deben realizarse *sin autorización* y *en perjuicio de tercero*; b) En inciso segundo, se tipifica la acción de acceder por cualquier medio a los datos personales y a quien los altere o utilice en perjuicio del titular o de un tercero.

Los tipos penales básicos podrán presentarse como agravados, siempre y cuando se tipifiquen las siguientes conductas:

a) Si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas. Este es un tipo penal compuesto (estructura típica doble), que requiere la previa comisión de uno de los tipos penales básicos del art. 197.1 y 197. 2 (apoderamiento de documentos electrónicos, al de control audio-visual telemático en forma clandestina y los relativos a los abusos informáticos contra el habeas data), según fuere el caso y previsto en el art. 197.3., como un tipo agravado de revelación, difusión o cesión a terceros de datos, hechos o imágenes;

b) Si se realizan por determinadas personas. Es el tipo agravado en razón a la esfera de dominio profesional del sujeto activo, según el art. 197.4, es decir, que tengan la condición de encargados o responsables de los bancos de datos (o *ficheros*), soportes informáticos, electrónicos o telemáticos, archivos y registros;

c) Si se revelan datos de carácter personal específicos. Es el Tipo agravado en razón de la afectación del *núcleo duro de la privacy*, es decir, contra los datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, según la primera parte del art.197.5;

d) Si la *víctima* fuere especial por su edad y/o aspecto sensorial. Es el Tipo agravado en razón de que la víctima sea un menor o incapaz, según la parte *in fine* del art. 197.5.

Estos dos tipos agravados (c y d), obedecen a una sana como acertada política criminológica de los Estados al proteger la esfera más íntima de la intimidad, no informatizables según las normas internacionales y recomendaciones europeas (Convenio de 1981 y Directiva 95/46/CE) y de reforzarla en el caso de los menores y personas con minusvalía.

e) Si se realizan contra el *núcleo duro* de la intimidad. Es el Tipo agravado en consideración a los fines de lucro perseguidos, según el art. 197.6 C.P, si conlleva la realización de los tipos anteriores (1 a 4 del art. 197). Si además, se realiza en atención a la conducta prevista en el art. 197.5, contra el *núcleo duro de la privacy*, se impone una *"pena hiperagravada de cuatro a siete años de prisión"*, según *Morales Prats* [38].

f) Si la autoridad o funcionario público realizara una *cualquiera de las conductas descritas en el artículo anterior* (197 CP. Se entiende entonces que no hay exclusión de ninguna modalidad delictiva), fuera de los casos previstos en la ley, sin que medie causa o investigación judicial por delito, y *prevaliéndose del cargo*. Es un tipo agravado en razón de la calidad del sujeto activo, prevista en el art. 198 C.P., y por tanto, con penas más severas. A esta norma se le han hecho varias críticas que las resumimos así: 1. Se considera innecesaria, pues hubiese sido suficiente con la aplicación de la agravante séptima del art. 22 del C.P.[39], sobre la prevalencia del carácter público que tenga el culpable; 2. Hacer referencia a cometer el hecho

---

(38) Ibídem, pág. 321
(39) SERRANO GOMEZ, Alfonso. ***Delitos contra la intimidad...*** pág. 235

fuera de los casos previstos en la ley *Aes meramente residual, pues se refiere a la falta de concurrencia de una causa de justificación"* [40] ; y, 3. Además de los *"defectos de coordinación sistemática* planteados por *Morales Prats"* [41], respecto del art. 198 y los arts. 535 y 356, sobre los delitos cometidos por funcionarios públicos contra la intimidad y siempre que haya mediado causa por delito, es evidente que las normas constituyen las dos caras de la transgresión a la intimidad por un funcionario público: con o sin causa por delito, pero con diferente graduación punitiva lo cual supone la aplicación del principio de favorabilidad sobre las penas a imponer.

4.2. En Colombia: Existen tipos delictivos en los que está presente la informática, electrónica y telemática como medios comisivos que atentan a la intimidad, la información, los datos personales y el habeas data; entre otros derechos y libertades fundamentales.

4.2.1. Tesis Negativa sobre la existencia del delito informático con base en el principio: *nullum crimen sine lege previa penale.*

Antes de la expedición del Código Penal de 1980 y aún hasta recientemente expedida la Ley 599 de 2000 se sostenía que no existe el delito informático como tal, 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* [42], 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 autonómica.

4.1.2. Tesis Ecléctica: Las nuevas tecnologías de la información y la comunicación o medios TIC, imponen una tutela penal y afectan al derecho de la información y los datos personales

Rivera Llano [43] , 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

---

(40) AA.VV. ***Código penal. Doctrina y jurisprudencia.*** Tomo II, Artículos 138 a 385. Dirección: Cándido Conde-Pumpido F., Ed. Trivium, S.A., 1a ed., Madrid, 1997. págs.2329 y ss.

(41) MORALES PRATS, F. Ob. ut supra cit., pág. 325

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

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

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.

Bajo estos supuestos la Ley 1273 de 2009, que reformó el C.P. colombiano del 2000, creó el bien jurídico protegido de la "Información y los datos" personales y en dos capítulos irrigó tutela jurídica. El primero, relacionado a "*los confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos*" y dentro de éste, los siguientes delitos (artículos 269 A a 269 G): (i) Acceso abusivo a un sistema informático; (ii) Obstaculización ilegítima de sistema informático o red de comunicación; (iii) Interceptación de datos informáticos; (iv) Daño Informático; (v) Uso de software malicioso; (vi) violación de datos personales; y, (vii) suplantación de sitios web para capturar datos personales. Además, se regula ocho causales de agravación punitiva aplicables a las anteriores conductas delictivas en el artículo 269 H, aunque algunas de ellas ya se encuentran inmersas en algunos delitos v.gr. el delito de violación de los datos personales, ya incorpora en el tipo, la causal de "provecho propio o de un tercero" que es la causal de agravación 5º.

En el Capítulo II, relativo a los "*atentados informáticos y otras infracciones*", previstos en los artículos 269 I y 269 J, están los delitos de "hurto por medios informáticos y semejantes" (se entiende por tales, los electrónicos y telemáticos); y el delito de "transferencia no consentida de activos.

4.1.3. Tesis positiva: Existencia del delito informático. Técnica Penal asimiladora de tipos.

Por su parte, el Criminólogo *Molina Arrubla* [44], al hablar de las diversas formas de la

---

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

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: 1) La *Criminalidad Retrógrada*, es decir, la referida al pasado, ubicando entre ellos los *delitos de Sangre*; y, 2) 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. El *delito informático* es en consecuencia, aquél se comete con el empleo de computadores o equipos electromagnéticos que transmiten datos o *informaciones* y afectan derechos y libertades fundamentales.

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..*" [45] .

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 aquéllos 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* [46] , 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.

El autor citado, al aplicar esta clasificación del delito informático alemana al caso colom-biano, comienza diciendo que el bien jurídico tutelado en estos casos prioritariamente es el

---

(45) TIEDEMANN, K., citado por Molina A. ob. ut supra., pág. 307
(46) Ibídem.

Patrimonio Económico (Título XIV del C.P.Col.), 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 C.P., 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" **[47]**, "*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*" (art. 3, lit., a Dec.1360/89), que justifica la protección jurisdiccional.

Más aún, con la expedición de la Ley 599 de 2000, se creó el bien jurídico tutelado de los "Derechos de Autor" **[48]** y se erigieron los siguientes delitos: (i) *Violación a los derechos*

---

(47) 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.

(48) 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 Decreto 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 omnicomprensivo, 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.

morales de autor (artículo 270); (ii) *Defraudación a los derechos patrimoniales de autor* (artículo 271); y, (iii) *Violación a los mecanismos de protección de los derechos patrimoniales de autor y otras defraudaciones* (artículo 272).

4.1.4. Tipos delictivos en los que está presente actualmente el fenómeno informático, electrónico y telemático. Bienes jurídicos de la "*La Intimidad*" y el "*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 el Código Penal de 2000 y en el Código Nacional de Policía en los artículos 46 a 49 y 56, al referirse a las contravenciones especiales contra la integridad personal y a la inviolabilidad de habitación o domicilio (Intimidad propiamente dicha e Intimidad domiciliaria).

Respecto de los delitos contra la Intimidad, el Código Penal del 2000, reformado la ley 890 de 2004, adicionó al bien jurídico tutelado de la reserva e interceptación de comunicaciones, la intimidad en el Capítulo VII, del Título III, de los delitos contra la libertad individual y otras garantías. En consecuencia, el Capítulo VII, hoy expresamente protege la "Intimidad" no solo como derecho fundamental sino como bien jurídico tutelable tanto a las personas individualmente consideradas como a la familia.

En consecuencia el Código Penal Colombiano vigente, para proteger la intimidad de las personas, regula las siguientes conductas delictivas: 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) *Violación ilícita de comunicaciones o correspondencia de carácter oficial* (art.196); y, 5) *Utilización ilícita de equipos transmisores o receptores* (art.197). Pero también, existen otros tipos penales que aunque no estén expresamente bajo el nomen iuris de la Intimidad como bien jurídico protegido, tácitamente si lo están porque hacen parte de aquella. Eso para con el delito de inviolabilidad de habitación ajena, sitio de trabajo, bien sea cometidos por particulares o servidores públicos y previstos en los artículos 189 a 191 del Código Penal. Aquí se protege la Intimidad domiciliaria.

El bien jurídico del derecho fundamental del "*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 (art. 15 Constitución Colombiana), 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) **[49]**, en bancos de datos de carácter público o privado

---

(49) "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. Igualmente, RIASCOS GOMEZ, Libardo O. ***La Constitución...*** ob. cit. págs.127 a 224.

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" (art. 74 Constitucional), es decir, el C.C.A., y la Ley 57/85, 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 (art. 20) como derecho fundamental de toda persona en los términos que la legislación universal lo ha instituido (Art. 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*" (arts. 20), como derecho genérico y la libertad de expresión o "*prensa*" (art. 73) y el derecho de toda persona de acceder a los documentos públicos, salvo las excepciones de ley (art.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 limite y autolímites que debe observar con respecto a los demás derechos y libertades constitucionales. En consecuencia, el art. 15 de la Constitución Colombiana, siguiendo los pasos de la Constitución Portuguesa (art. 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 iusfilósofo *Pérez Luño*, [50] con la llamada "*Libertad informática*", escindida del art. 18.4 CE., que regula la informática como límite al ejercicio los derechos fundamentales, como la intimidad, honor, imagen, etc..

Otra interpretación diferente es la que se dio por parte del constituyente colombiano en la Constitución de 1991, al incorporar antitécnicamente 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

---

(50) PEREZ LUÑO, Antonio Enrique. ***Derechos humanos, estado de derecho y constitucional.*** Ed. Tecnos, Madrid, 1984. págs.359 y ss.

complementarios e inseparables y esto no es del todo así.

La Corte Constitucional Colombiana, paulatinamente va desentrañando la autonomía del derecho de *habeas data* y la intimidad, como veremos ut supra [51], 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"* [52] 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 géneris*, 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 [53] 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 iusinformática ha planteado sus diferencias de contenido, alcance socio-jurídico y carácter proteccionista por parte del Estado [54].

Esta técnica *sui géneris* 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 enten-

---

(52) Vid. Corte Constitucional: Sentencia C-114, Marz.25 de 1993. Sala Plena. Ob.cit. pág. 428.

(51) Vid. Corte Constitucional: Sentencias: 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.

(53) 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 de "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.

(54) Por el contenido, se tiene la dificultad para delimitar el verdadero contenido de la intimidad, por contra al del habas 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´ A). "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.

der 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 aquéllos se reputan no por su mera ubicación formal en la Constitución, ni por ser de aplicación inmediata (art. 85 Constitucional), o ser objeto de "*Acción de Tutela*" (art. 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 [55].

La Ley 1273 de 2009, reformatoria del C.P., del 2000, al crear el bien jurídico de "la protección a la información y a los datos" personales y erigir nueve (9) tipos penales contra la confidencialidad, integridad y disponibilidad de los datos y los sistemas informáticos, de un lado, y contra los atentados informáticos y otras infracciones, de otro, no hizo más que elevar a rango de bien jurídico tutelable la información y el habeas data, entendido éste derecho constitucional autónomo del derecho a la intimidad como veremos más adelante, como el derecho que tiene toda persona a solicitar que sus datos sean recolectados con consentimiento a quien concierne, así como a solicitar la actualización, rectificación o eliminación de los datos cuando sean ilegales, falsos o incompletos dentro o fuera de cualquier procesamiento de datos (informático o manual) que incluye varias etapas: recolección, almacenamiento, registro y transmisión de datos.

Desde este punto de vista, los nueve tipos delictivos básicos y agravados --como veremos más adelante en detalle--, previstos en los artículos 269 A a 269 J del Titulo VII Bis del Código Penal colombiano, protegen no solo el derecho a la información sino el derecho constitucional de Habeas Data que tiene toda persona para proteger sus datos o informaciones que le conciernen, según el artículo 15 y en concordancia con los artículos 20 y 74, constitucionales.

---

(55) Sentencia 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.

II. LOS DELITOS CONTRA LA INTIMIDAD

1. LA INTIMIDAD Y LA INFORMÁTICA EN LA CONSTITUCIÓN DE 1991

El Derecho a la intimidad en las Constituciones democráticas de la segunda mitad del presente siglo, 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 las Constituciones de España de 28 de Diciembre de 1978, art. 18 (CE) y en la Constitución Política de Colombia de 1991, art. 15 (C.P.)

El derecho a la intimidad en la actual Constitución, ratifica que éste es un derecho inherente a la persona humana y como tal inalienable, inenajenable e imprescriptible, que las autoridades instituidas en la República protegen y garantizan a todas las personas residentes en Colombia (art. 2º C.P.).

El proceso de evolución conceptual, tanto de la intimidad, como de los actuales derechos fundamentales [1] y del Estado mismo, son fruto de una incesante e inacabada teorización basada en las prácticas, usos, costumbres y regulaciones normativas de los diferentes pueblos de la tierra y, por supuesto, del trabajo intelectual de la doctrina y jurisprudencia iusuniversales. Por eso, en el siglo XXI, hemos decantado al derecho de la intimidad personal y familiar como un derecho fundamental de la persona humana, elevado a rango constitucional como derecho autónomo pero limitado por otros derechos de igual jerarquía, por el ordenamiento jurídico y por una serie de intereses, valores y principios igualmente constitucionales; pero por sobre todo, se ha considerado también al derecho a la intimidad como un derecho digno de excelsa protección por parte del Estado y de los particulares mismos, ante los pluriofensivos riesgos jurídico-tradicionales así como los devenidos recientemente por los avances tecnológicos de la información y la comunicación (conocidos como fenómeno TIC [2]) unidos a los penetrantes, porosos y complejos desarrollos de la informática, electrónica y telemática.

---

(1) Véase, especialmente los comentarios del surgimiento y evolución del artículo 10 de la CE, catalogado como "la piedra angular de todo el sistema jurídico que ella (se refiere a la Constitución Española) instituye", pues junto al análisis y evolución del art. 18.4 CE., constituyen el epicentro del presente ensayo jurídico en entronque con las ciencias informáticas, electrónicas y telemáticas RUIZ-GIMENEZ CORTEZ, Joaquín. ***El artículo 10. en: comentarios a la Constitución española de 1978***. Cortes Generales. Ed. Derecho Unidos. Madrid 1997, p.39 y ss.

(2) Estas nuevas tecnologías TIC, que surgieron inicialmente de las denominadas por el profesor *Ethain Katsh*, "tecnologías de la información TI", no son sólo aquellas "que se llevan a cabo con los simples artefactos funcionales, sino que constituyen verdaderas nuevas formas de recibir y transmitir información de forma más interactiva y permite recoger, seleccionar, organizar, almacenar y transferir cualquier cantidad de información de un sitio a otro, sin frontera geográfica alguna y a velocidades y formatos electrónicos". Quizá por estas amplias capacidades de transmisión electrónica (emisión/recepción) en la que se basan las nuevas tecnologías de la comunicación, es por lo que estos fenómenos pueden calificarse de novísimas tecnologías TIC, adicionando a ese bien intangible, poderoso, poroso, penetrante, de difícil control (jurídico, tecnológico, personal y social) y de incalculable valor económico como es la *información* actualmente, el vehículo electrónico idóneo, sin el cual aquella pierde parte de su magia y estructuración, como lo es, la comunicación a través de medios eléctricos, informáticos, electrónicos y telemáticos. Nuestros Trabajos: (i) ***La Constitución de 1991 y la informática jurídica. ed. uned***, Pasto, pág. 7 y ss; (ii) ***La visión ius-informatica de la intimidad y los delitos relativos a los datos personales.*** Tesis Doctoral, Universidad de Lleida (España), Mayo de 1999. También en KATSH, Ethain. ***Rights, camera, action: cyberspatial settings and the firts amendment***. Texto Original en inglés en la dirección electrónica: *www.umontreal.edu.ca*

El derecho a la intimidad, en su evolución conceptual ha pasado por diversas definiciones. En efecto, desde el célebre ensayo "The right to privacy" de Warren y Brandeis de 1890 en el cual la "privacy" se tenía como el derecho a ser dejado en paz, a vivir libre de toda injerencia externa por parte de otras personas a no poder circular o publicar sin el consentimiento del titular fotografías o imágenes de aquel, hasta que con el paso de los años nuevas formas mecánicas y tecnológicas cambiaron las técnicas de injerencias o invasión a la privacidad (más amplia o genérica) o la Intimidad (especie de la privacidad según varios autores ibéricos). Así comenzó a definirse a la intimidad como el derecho a poder controlar la información personal sobre sí mismo (igual *Parker* en 1974 y *Fried* en 1979, *De Miguel* en 1983, *Fariñas* en 1984*, O´Callaghan* y *Pérez Luño* en 1984).

Según los doctrinantes, el derecho a la intimidad es un derecho de la persona (*Battle Sales,1972*), que fomenta y desarrolla la personalidad (*Bajo Fernandez,1980*), inherente a la zona espiritual o interior (*Desantes,1972*), con atributos y poderes (*Albadalejo,1979*), para oponerse a lo público (*Urubayen,1977)* para exigir la no intromisión, indiscreción ajena (*Castán*), vistas, escuchas y captaciones de datos personales (*López Jacoiste,1988*), por cualquier medio tecnológico de la información y la comunicación o medios TIC y/o informático (*Riascos Gómez, 1990*) y referido a sus relaciones consigo misma o con algunas otras muy cercanas a él, mujer, hijos, padres, algunos amigos, que le rodean en su vida *(Urubayen*), es decir, es un derecho de la persona y de la vida familiar (Constituciones Española, Portuguesa y Colombiana).

En esta época de evolución del derecho a la intimidad, surgen la mayor parte de Leyes protectoras de este derecho en forma autónoma e independiente de otros derechos, aunque no del todo liberadas de la protección conjunta con el derecho al honor, la propia imagen y el buen nombre, como sucedió en España, con la expedición de la Ley Orgánica 1º de 1982. Sin embargo, a partir de la década de los años 70, la irrupción de la protección de la protección de la intimidad en todos los ámbitos de la vida cotidiana, la universalización del contenido, se pone en evidencia con mayor fuerza la inusitada aceleración y desarrollo de las nuevas tecnologías de la comunicación y la información (TIC) al abrigo de la informática que tenia la virtualidad de tratar informaciones o datos (*unidades de información codificada por medios electromagnéticos*) de todo tipo. Surge el temor para unos y la visión de evolución para otros del derecho de la intimidad. Comienza a hablarse de la intimidad como un derecho al autocontrol de la información de una persona, el control de la información del concernido, etc. Con este ambiente evolutivo de la intimidad, surge las leyes Suecas, norteamericanas, alemanas, Danesas, Suizas, francesas e Inglesas, que las llaman de "protección de la privacy", "Protección de los datos", "relativa a la informática y los derecho y libertades", etc., todas ellas producidas entre 1973 a 1984.

En Colombia en 1976, se expiden en un ámbito sectorial dos Decretos-leyes y una Resolución reglamentaria del Departamento Administrativo Nacional de Estadística (DANE), por los cuales se "*dictan normas sobre utilización de sistemas de información y de equipos y servicios de procesamiento de datos*" en el sector público, y que entre otros objetivos tenía, los proteger y garantizar los derechos y deberes de los contratistas con el Estado, en los cuales se utilicen sistemas, equipos y medios computacionales, informáticos, electrónicos o telemáticos.

El espíritu que rondaba en aquellas normas no era otro que el de proteger o garantizar derechos de la persona, como la intimidad, que pudieran verse vulnerados en el proceso de contratación administrativa, comercial o civil con el Estado, aunque no se hubiese planteado la intimidad en forma explícita, esta se deduce pues el temor universal por aquella época era el riesgo y la vulnerabilidad que fantasmagóricamente rondada en el ambiente público y privado

con la llegada de las nuevas tecnologías de la información y la comunicación apoyadas por la informática y las cuales representaban un filón de mucho cuidado para quebrantar derechos de la persona humana. Los nuevos fenómenos tecnológicos TIC y la informática de labios hacia afuera han representado un gran avance para la humanidad, pero hacia el interior (en el ámbito privado, y sobre todo público) un leviatán que sigue creciendo desde mediados del siglo XX y tras su crecimiento y consolidación sigue produciendo nuevas y variadas formas de temor, riesgo y porosidad.

Sin embargo, pasaría otros cuantos años más para que la intimidad se elevara a rango constitucional en el artículo 15 de la Constitución de 1991, donde se garantizó a toda persona el derecho a la intimidad personal y familiar a través del mecanismo constitucional de la acción de tutela (art.86 Ibid), por ser un derecho fundamental de aplicación inmediata que no necesitaba reglamentación general o especial para ser protegido por los jueces de la república y ha sido precisamente la jurisdicción constitucional, la que jurisprudencialmente ha ido perfilando el alcance del derecho a la intimidad, su ámbito y mecanismos de protección judicial, los sujetos legitimados para reclamar la protección a la intimidad y los obligados a respetar y protegerla, así como los entronques o posibles conflictos con otros derechos y libertades fundamentales (información y libertad de prensa, habeas data, buen nombre, inviolabilidad de comunicaciones y domicilio, etc.). Por eso se afirma, que la evolución conceptual del derecho a la intimidad en Colombia ha sido jurisprudencial con algunos lunares legislativos.

Quizá por esta razón, es por lo que no existen leyes de estirpe ius civilista o administrativa en nuestro país que protejan y garanticen *in integrum* el derecho a la intimidad, aunque sí leyes sectoriales y dispersas que plantean mecanismos de defensa jurídica de la intimidad de las personas de las diferentes injerencias, ataques o invasiones a la vida privada o íntima, en forma directa (Ley 559 de 2000, reformada parcialmente por la Ley 890 de 2004) o indirecta (Código Contencioso Administrativo, Ley 57 de 1985, Ley 190 de 1995, Ley 527 de 1999, Ley 962 de 2005, Ley 1266 de 2008, Ley 1341 de 2009, entre otras), como precisaremos más adelante.

La informática [3] se ha entendido, como la capacidad potenciada con medios informáticos, electrónicos y telemáticos (v.gr. elementos, aparatos y sistemas computacionales y de comunicación electrónica: la telemática y la multimedia) utilizados en el tratamiento logicial o mediante sistemas de tratamiento de **E**ntrada (E: ***I****nput*) o **S**alida (S: ***O****utput*) de cualquier cantidad o clase de información [4] generada por el ser humano en sus diversas actividades o profesiones. Información, en tanto en cuanto, sea considerada como un bien con valor

---

(3) *Vittorio Frosini* (En: Informática y Derecho), comenta como surgió el término "informática" de la definición dada por *Philippe Dreyfus*, en los siguientes términos: "L´informatique est la science du traitement rationnel, notamment para machines automatiques, de l´information considerée comme le support des connaissances et des communications dans les domaines technique, économique et social". Y fue también a partir de esta concepción de informática, que las diferentes Leyes de Protección de los Titulares de los Datos Personales en la Unión Europea (UE), como en los diferentes Estados que la componen, que se hizo institucional el término de "*tratamiento automático*" de la información o datos de carácter personal. Terminología técnico-jurídica que aún subsiste, a pesar de corresponder a la etapa de surgimiento de la computación y de los ordenadores donde se destacaba una de las funciones primarias de aquellas máquinas, cual es, la automatización de datos, tal como lo hace hoy un cajero electrónico. Mi trabajo. ***La Constitución de 1991 y la informática jurídica...*** Ob. cit., pág. 47 y ss.

(4) LOPEZ MUÑIZ-GOÑI, Miguel. ***Informática jurídica documental***. Ed. Diaz de Santos, Bilbao,1984, pág. 39.

con valor económico [5], social y jurídico y sea posible transferirla (emitir y recepcionar) de un lugar geográfico a otro, a velocidades, con equipos y formatos eléctricos y electrónicos (comunicación por cable y electrónica: telemática y multimedia [6]) y posean una finalidad y objetivos predeterminados.

La informática jurídica o *iusinformática*, hace referencia al tratamiento lógico, con soportes, equipos y medios eléctricos y electrónicos de la información o datos generados por el hombre en el ámbito social y jurídico.

La iusinformática es entonces, una parte especializada de carácter académico y sectorial de la informática general que día a día cobra capital importancia, porque a ella hay que referirse en la aplicabilidad de una coherente técnica legislativa con los nuevos fenómenos tecnológicos TIC y la informática tales; entre otros, como: a) En la regulación de los derechos y obligaciones consecuentes de la creación, distribución, explotación y/o utilización del hardware y software, con su protección en los derechos de propiedad industrial o en los propiedad intelectual; b) En la regulación de los derechos y obligaciones de los creadores, distribuidores y usuarios de bases de datos jurídicos (o "*ficheros*", según la terminología francesa y española); c) En la contratación de bienes y servicios informáticos; d) En las "Leyes protectoras de Datos Personales" y la potencial no sólo agresividad, sino defensabilidad que representa, según el caso la informática; e) La estructuración y regulación normativa de los denominados "*delitos informáticos*" [7], bien sean los cometidos con medios informáticos, electrónicos o telemáticos, o bien los cometidos contra los datos personales en el ámbito del proceso de sistematización –recolección, almacenamiento, registro y circulación, transmisión o "flujo" de datos- o contra el hardware o software informático; f) la regulación del ejercicio, protección y garantía de los derechos y libertades fundamentales de la persona humana (el "honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos", art. 18.4 CE); y g) La regulación de los derechos estructurales del derecho de *habeas Data* (acceso, actualización, rectificación y cancelación de la información), posteriores a los derechos de notificación e información ("derecho a conocer") que ostenta el titular de los datos que le conciernen en un sistema de tratamiento (recolección, almacenamiento, registro, conservación y "circulación de datos") informatizado y aplicable al conjunto de derechos y libertades fundamentales previstos en la Constitución

---

(5) En el ámbito punitivo español como en el colombiano, siguiendo las tesis alemanas de Tiedemann, al proponer la tesis de creación del bien jurídico denominado de la "información", siempre que sea tenida como bien con valor económico, para referirse a los llamados delitos informáticos. Vid. GUTIERREZ FRANCES, María Luz. ***Delincuencia económica e informática en el nuevo código penal***.. En: Cuadernos de Derecho Judicial. Escuela Judicial. C.G.P.J. No. XI, Madrid, 1996. Además, ***Notas sobre la delincuencia informática: atentados contra la "información" como valor económico de empresa***. En: Estudios de Derecho Penal Económico. Editores: Luis Zapatero y klaus Tiedemman. Ed. Univ. de Castilla-La Mancha. Tarancon (Cuenca). 1994, pág. 183 a 208.

(6) La multimedia es una de las formas de comunicación electrónica realizada a través de elementos, sistemas y equipos computacionales, por los cuales se transfiere (emite/recepciona) cualquier tipo de información o datos contenidos en formatos de texto, imágenes y sonido.

(7) Por éstos y otros supuestos que amplía la lista, es por lo que el Davara, estima que la iusinformática, hoy por hoy, bien puede configurar una nueva rama del derecho, el *Derecho Informático*, en el que todos los juristas estamos comprometidos a Atrabajar para colaborar en marcar bien claramente las diferencias entre lo que es, lo que puede ser y lo que debe ser, orientando el camino que debe tomar la regulación jurídica del fenómeno informático en la hemos dado en llamar el "Derecho Informático". Nosotros creemos haber aportado algo a esa estructuración en el trabajo *ut supra* citado. DAVARA RODRIGUEZ, Miguel A. ***Manual de derecho informático***. Ed. Aranzadi S.A., Pamplona, 1997, págs. 25 a 41.

Colombiana [8], la Constitución Portuguesa [9] y la Constitución del Brasil [10].

Por la necesidad cada día mayor del derecho de regular materias del conocimiento humano, sobre todo las de índole tecnológico surgidas de la llamada informática, para que sean creadas, desarrolladas, protegidas, garantizadas y utilizadas conforme a un ordenamiento jurídico en vigor, es por lo que el profesor *Hernández Gil,* citado por *Davara*, al hablar de los problemas socio-culturales de la informática jurídica, estima que el derecho *strictu sensu* no va a ordenar nuevas realidades, sino que el Derecho mismo va a experimentar, en cuanto objeto de conocimiento, una mutación, derivada de un modo distinto de ser elaborado, tratado y conocido.

Sin embargo, dicha experimentación es de tal entidad que la informática necesita del derecho, como el derecho de la informática, tal y como lo sostienen *González Navarro* y *Lasso de la Vega* [11], que resulta insuficiente la estricta observación pasiva de los juristas por lo que

---

(8) La Constitución de 1991, en el art. 15, inmerso en el Título II, Cap.I., "De los Derechos Fundamentales", expresa: "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, tienen 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....". Aunque el derecho de habeas data está inmerso en el de la intimidad, no debe interpretarse en forma miope que sólo a éste es aplicable, sino que por la ubicación sistemática no simplemente formal, la garantía y protección constitucional se reputa para el conjunto de derechos considerados fundamentales. El error de la ubicación temática del habeas data por parte de la Comisión Codificadora de la Constituyente de 1990, no debe conducir a la negación o, más aún, la evaporación de las garantías y mecanismos constitucionales de protección del conjunto de derechos fundamentales. El Constituyente Colombiano debió beber íntegramente de las fuentes de donde trasplantó parcialmente el art. 35 de la Constitución Portuguesa (que regula la "Utilización de la Informática" en el contexto del Título II, Cap. I. "Dereitos, libertades e garantias pessoais), a fin de que no aparezca un artículo 15 (Derecho a la Intimidad) fusionado con el de habeas data y generando, --lo que es aún peor-- una forzada y casi inseparable dependencia.

(9) El Titulo II, Dereitos, Libertades e garantias, Cap.I, Art. 35 (Utilizaçâo da informática). Por la ubicación formal y sistemática del citado artículo se deduce que el derecho de habeas data como la limitación al uso de la informática se aplica al conjunto de derechos y libertades fundamentales. Citamos a continuación el texto normativo conforme a la reforma introducida al art. 35, según la LC Núm. 1/1982, pues el texto original de la Constitución de 1976 que constaba de tres numerales fue reformado, aunque el espíritu y gran parte del texto de aquella se mantuvo. La mentada norma expresa: 35-1. Todos los ciudadanos tendrán derecho a tener conocimiento de lo que consta en forma de registros informáticos que les conciernen y de la finalidad a la que se destinan esas informaciones (datos o registros), y podrá exigir, llegado el caso, la rectificación de los datos, así como su actualización. 35-2. Está prohibido el acceso de terceros a los ficheros (o banco de datos) con datos personales o a la respectiva interconexión de aquéllos, a través de los flujos transfronterizos, salvo en las casos exceptuados en la ley (Inciso nuevo). 35.3 La informática no podrá ser utilizada para el tratamiento de datos referentes a las convicciones filosóficas o políticas, a la filiación partidista o sindical, a la fe religiosa o la vida privada, salvo cuando se trata de procesamiento de datos no identificables individualmente para fines estadísticos. 35-4. La ley definirá el concepto de datos personales para efectos de registro informático (nuevo). 35-5. Se prohíbe la atribución de un número nacional único a los ciudadanos. Los paréntesis de la norma son nuestros, así como los giros de traducción no literal del portugués. Texto Constitución Completo en: **AA.VV. *Constituçao novo texto***. Coimbra editora, Ediçao organizado JJ. Gomes Conotilho o vital M., 1982

(10) Así lo confirman, los profesores *González Navarro y González Pérez*, siguiendo a *Heredero Higueras*, al recordar que la Constitución brasileña de 1988, incorporó el su texto el derecho de *habeas data* que inicialmente sólo se atribuía al derecho que tenía toda persona para acceder a la información que le concernía al considerarse "una modalidad de acción exhibitoria análoga a la del habeas corpus". Hoy en día, la estructuración y ampliación del contenido de aquél derecho, conlleva a extender las facultades iniciales de dicho derecho a otras, tales como los de actualización (o la puesta al día *--up date anglosajón--* de los datos), rectificación y cancelación de los datos personales que le conciernen a una persona, sí los datos fueren inexactos, incompletos o ilegales. Vid. GONZALEZ NAVARRO, F. Y GONZALEZ PEREZ, J. ***Comentarios a la ley de régimen jurídico de las administraciones publicas y procedimiento administrativo común****.* Ed. Civitas, 1a., ed., Madrid, 1997, pág. 711.

(11) Vid. GONZALEZ NAVARRO, Francisco. ***Derecho administrativo español****.* Ed. Eunsa (Univ. de Navarra), Pamplona, 1987, pág. 190-194.

sólo la iusinformática puede aportar al derecho, si éste a su vez, no suministra sus técnicas, métodos y procedimientos que lo catalogan como ciencia social del conocimiento humano para comprender la dialéctica que se está produciendo en su interior, tras el advenimiento de las nuevas tecnologías TIC en unión con la informática, hasta tal punto que, hoy hablamos de un *Derecho informático,* impensable décadas de años atrás.

1.1. El Caso Samuel Warren y Louis Bandreis. "The right to privacy" de 1890 [12] .

Los variados mecanismos de protección jurídica (civil, administrativo, laboral, constitucional y penal) del derecho fundamental de la intimidad personal y familiar, implementados hoy por hoy, por los diferentes países europeos y americanos hacía impensable imaginarlos, hace más de un centenario cuando que produjera el famoso precedente doctrinal y jurisprudencial norteamericano, a partir del ensayo de los abogados *Warren y Brandeis* de 1890, sobre "The right to privacy" aparecido en la Revista de Derecho de Harvard.

El Derecho a la Intimidad, o en su origen angloamericano *The Right to Privacy*, surgió en una intromisión o injerencia periodística en la "privacy" de un famoso personaje de la vida social y política norteamericana del siglo pasado en unos ambientes históricos, sociales, culturales, étnicos, políticos e incluso de concepción y estructuración, tan disímiles en tiempo, espacio y aún conceptuales de lo que hoy entendemos en líneas generales por *privacy* [13] o por intimidad.

Samuel Warren y Louis Brandeis, tras haber sufrido Warren en carne propia la vulneración de éste derecho (*The Right to Privacy*) con la publicación de las actividades personales y sociales mantenidas dentro y fuera de su hogar como repercusión de las escenas que protagonizaba en los sitios públicos y privados con su "vida de lujo y rumbosa". Actitudes que se agravaban por ser Warren el esposo de la hija de un prestigioso Senador de los Estados Unidos y porque Atrajo la curiosidad y la chismografía (chismorreo *o Gossip*) de los periódicos en sus crónicas amarillas, hasta el punto de suscitar escándalo".

Los juristas Warren y Brandeis, para estructurar *The Right to privacy* [14], parten del análisis de uno de los fundamentales principios del *Common Law,* que sostiene*: Todo Individuo debe gozar de total protección en su persona y en sus bienes*. Principio revisable como todos los que componen el Common Law por los constantes cambios políticos, sociales y económicos que surgen y se imponen en la misma sociedad que tuvieron origen. En el presente caso, la revisión posibilitó igualmente la redefinición de la naturaleza y extensión de dicha protección.

Los autores para llegar a preguntarse sí en aquella época existía o no un principio de C*ommon Law* que permita invocarse para amparar la privacy (intimidad), analizan los siguientes aspectos:

a) La evolución de las concepciones jurídicas, efectos y alcances de los derechos a la vida, a la libertad y a la propiedad que tiene toda persona;

---

(12) RIASCOS GOMEZ, Libardo O. ***El derecho a la intimidad, su visión iusinformática y los delitos relativos a los datos personales.*** Tesis doctoral, con calificación Excel.lent "Cum laude", Universidad de Lleida (España), 1999, pág. 10 y ss.

(13) LOPEZ DIAZ, Elvira. ***Derecho al honor y el derecho a la intimidad****. Jurisprudencia y Doctrina.* Ed. Dykinson, Madrid, 1996, pág. 197.

(14) Para las glosas y comentarios del Ensayo Warren y Brandeis, seguimos *ad pedem litterae*, la traducción de Pendás y Baselga. PENDAS, Benigno y BASELGA, Pilar. ***El derecho a la intimidad. (the right to privacy)***. Ed. Civitas, Madrid, 1995.

b) La Sentencia del Juez *Cooley* (1888), sobre el denominado derecho "*a no ser molestado*"[15], cuando se la invaden "los sagrados recintos de la vida privada y hogareña", con la toma de fotografías por parte de empresas periodísticas sin el consentimiento de los fotografiados; y,
c) El escrito de *E.I Godkin*, sobre *The Rights of the Citiezen: To his Reputación* de junio de 1890, en donde evidencia el peligro de una invasión de la intimidad por parte de los periódicos de la época, sobre todo, cuando hacía comentarios sobre la vida personal y familiar de los ciudadanos en detrimento de su reputación, poniéndolas "en ridículo" o violando "su intimidad legal" [16].

Los cambios políticos, sociales y económicos imponen el reconocimiento de nuevos derechos y el Common Law evoluciona para dar cabida a las demandas de la sociedad. Así, los derechos a la vida, a la libertad y la propiedad de las personas, como otros, están evolucionados por dichos cambios y demandas. En efecto, la vida que sólo se protegía de las diferentes formas de violencia, hoy significa el derecho a disfrutar de ella, a no ser molestado. La libertad, ser libre no sometido, a un derecho a la libertad que garantiza un amplio haz de derechos subjetivos; y la propiedad de bienes materiales, hoy abarca tanto a bienes tangibles como intangibles.

En efecto, la evolución significó el reconocimiento legal de las sensaciones, los pensamientos y las emociones humanas, tras reconocer paulatinamente la extensión de la protección contra daños físicos de la mera prohibición a causarlos a la de poner a otro en peligro de sufrirlos (acción de amenazas y, mucho más tarde, a la protección del individuo contra los ruidos y olores desagradables, contra el polvo y el humo y las vibraciones insoportables: el derecho sobre actividades nocivas y molestas tomaba cuerpo).

Las emociones humanas se ampliaron al ámbito de la inmunidad personal más allá del propio cuerpo. Se tomó la buena fama, la protección social (leyes de difamación y libelo). Las relaciones de familia del hombre se convirtieron en parte del concepto legal de su vida, y la pérdida del cariño de la esposa se consideró un daño compensable. En fin, se reconoció los daños y perjuicios por atentado contra los sentimientos de los padres. De la propiedad material surgieron los derechos inmateriales que resultan de ésta, los llamados productos y procesos de la mente, tales como las obras literarias y artísticas, los secretos industriales y las marcas comerciales.

El Juez Cooley denominó derecho *a no ser molestado* (The Right *to be let alone*), el amparo a la persona de "los recientes inventos" (fotografía) y los nuevos métodos de hacer negocios. Las fotografías y las empresas periodísticas han invadido los sagrados recintos de la vida privada y hogareña; y los numerosos ingenios mecánicos amenazan con hacer realidad la profecía que reza: "lo que se susurre en la intimidad, será proclamado a los cuatro vientos". Desde tiempo atrás se esperaba que un recurso impida la circulación no autorizada de retratos de particulares.

---

(15) (16) *The right to be let alone,* ha significado para autores como *Vittorio Frossini*, (Ob.cit., pág. 64) --y desde allí *et all*-- el *summun* o la esencia del derecho a la intimidad en sus orígenes. Sin embargo, como vemos en este planteamiento silogístico del trabajo Warren y Brandeis, apenas significa un elemento, importante sí, pero no el único y a manera de primera premisa, de lo que debemos entender integralmente por el derecho a la *privacy* (la intimidad, que es el término que engloba y más fielmente refleja el concepto de privacy): su características, sus límites como derecho no absoluto, sus colisiones y toma de elementos de otros derechos como el del honor o la propiedad intelectual y artística; y en fin, sus mecanismos de reparación o indemnizatoria en caso de daños. Más aún, así se evidencia en el propio ensayo de Warren y Brandeis, se lee: "*La soledad y la intimidad* se han convertido en algo esencial para la persona; por ello, los nuevos modos e inventos, al invadir su intimidad, le producen un sufrimiento espiritual y una angustia mucho mayor que la que le pueden causar los meros daños personales". Cfr. PENDAS, B., y BASELGA, P. Ob. cit., págs. 25

The Right to be let alone [17]. Este derecho a no ser molestado significaba, para aquella época, no sólo un factor negativo --como es la posición doctrinaria más difundida actualmente--, sino también un factor positivo, basada en no dejar circular las fotografías de una persona (La fotografía, era un invento mecánico que invadía abierta y subrepticiamente la vida privada de las personas) sin consentimiento del titular.

Sin embargo, la invasión en la intimidad, por los periódicos se evidenció tras el escrito de E.I. *Godkin* en Julio de 1890. Un mes atrás, un Tribunal de New York había reconocido a la prohibición a la circulación de retratos sin el consentimiento del fotografiado (Caso *Marion Manola* Vs. *Stevens & Myers*. Junio 1890). Por todo ello, se impone, la necesidad de una protección más amplia de la persona. "La prensa esta traspasando, en todos los ámbitos, los límites de la propiedad y la decencia. El chismorreo ha dejado de ser ocupación de gente ociosa y depravada, para convertirse en una mercancía, buscada con ahínco e, incluso, con descaro".

Todavía hoy, estos aspectos de forma, ambientales y aún geográficos sirven de base para ampliar la conceptualización o manifestaciones de ese derecho único que es la Intimidad, pues el paso del tiempo nos ha servido para universalizar aquél derecho, para enriquecerlo con sus diferentes manifestaciones o visiones, para legalizar o constitucionalizarlo entre los Estados con derecho escrito como el Español y Colombiano, sin olvidar el precedente angloamericano en sus orígenes, en su estructuración teórico-práctica y sus posibilidades de enriquecimiento con el paso de los años, los espacios geográficos o los avances tecnológicos, como los sobrevenidos a mediados del siglo XX y conocidos como TIC.

En tal virtud, para estructurar la visión iusinformática del derecho a la intimidad, partimos del precedente norteamericano de 15 de diciembre de 1890 [18], pues a partir aquí se comienza a delinear *The Right to privacy,* como un derecho de la persona humana, diferente a los demás derechos existentes (patrimoniales o extrapatrimoniales), aunque retome elementos y características de algunos otros como el de propiedad, el derecho a la vida o valores constitucionales como la *inviolabilidad y dignidad de la persona* para explicarlo y estructurarlo, sin confundirlo con ellos. Así mismo, partimos del precedente, pues desde aquél entonces ya se vislumbraba la visión iustecnológica de la intimidad, cuando en las decisiones del

---

(17) En el sentido expuesto por Frossini (nota 26), se sostiene que :"Samuel D. WARREN y Louis D. BRANDEIS, ... exponen, ... las bases técnico-jurídicas de la noción de privacy, configurándolo como un derecho a la soledad, como la facultad de "*to be let alone*" (el derecho a estar solo, o mejor, el derecho a ser dejado tranquilo y en paz), uniéndose en esta expresión --que cobra carta de naturaleza-- a lo llamado, anteriormente en 1888, por… COOLEY, "The Right to be let alone". Este derecho a no ser molestado significaba, para aquella época, no sólo un factor negativo, sino también un factor positivo, basada en no dejar circular las fotografías de una persona (La fotografía, era un invento mecánico que invadía abierta y subrepticiamente la vida privada de las personas) sin consentimiento del titular. Estos planteamientos, fueron plasmados judicialmente, como lo asevera la autora citada, al decir que "Tres años más tarde de la publicación de este conocido artículo un Tribunal utilizó por primera vez la expresión acuñada por los dos abogados, Warren y Brandeis, fue el caso MARKS V. JOFFA, fallado por el Tribunal de New York: el demandante, un actor y estudiante de leyes, había visto un retrato suyo publicado en un periódico propiedad del demandado, formando parte de un concurso de popularidad, al que se le oponía personalmente. La sentencia, estimó la demanda y declaró su "derecho a ser dejado en paz", basándose en el hecho de que "ningún periódico o institución tiene derecho a usar el nombre o la fotografía de nadie, sin su consentimiento": Cfr. LOPEZ DIAZ, Elvira. ***El derecho al honor y el derecho a la intimidad.*** Ed. Dykinson, Madrid, 1996, pág. 175

(18) Tendremos en cuenta la obra clásica de la literatura jurídica aparecida en el famoso opúsculo de Samuel WARREN y Luois BRANDEIS, denominado: "The Right to Privacy" ("privacy": Término polémico en su traducción al castellano porque se le ha querido dar diversas connotaciones jurídicas que no tienen en su origen anglosajón, según sea intimidad, privacidad o vida privada, tal como veremos a lo largo de la investigación). El artículo con aquél nombre apareció en la *Harvard Law Review,* Vol. IV., núm. 5, de 15 de diciembre de 1890. ***El derecho a la intimidad.*** Trad. PENDAS, Benigno y BASELGA, Pilar., Ed. Civitas, S.A., 1a ed. Madrid, 1995.

Tribunales Norteamericanos recogidas en el Ensayo de Warren y Brandeis se proscribía *las injerencias en la privacy con aparatos fotográficos* ("cámaras de fotografía") *o* producto de los *avances de la tecnología* ("recientes inventos"). Se vislumbra desde aquél entonces una puerta visional del ámbito *iusinformático,* a través de los recientes inventos y como una manifestación más de un único derecho: *The Right to Privacy* o derecho a la intimidad.

Con este proceder no pretendemos desconocer la "evolución histórica del derecho de la intimidad", relatada a través de las diferentes etapas de la humanidad en forma magistral por *Fariñas* [19] y fundadas en lo que hoy constituyen los elementos intrínsecos y extrínsecos de la intimidad, de otras de sus manifestaciones o de derechos autónomos de la persona humana (sentimientos, recuerdos, hogar, vida privada, interioridad humana, daño moral, aspectos corporales o incorporables --v.gr. datos personales--, relaciones familiares, paz y sosiego personal y familiar, honra, domicilio, el honor, la buena imagen, el nombre, etc.), sino delimitar en el tiempo y en el espacio nuestro ensayo, tener un referente universal *ab initio* que permita el fundamento teórico-práctico de nuestro planteamiento.

2. LA INTIMIDAD COMO BIEN JURÍDICO TUTELADO

2.1. Protección jurídica sustantiva y procesal de la intimidad en el derecho civil, administrativo, punitivo (delictual y contravencional) y en el derecho internacional.

El derecho a la intimidad personal y familiar, en la Constitución Colombiana como la Española, es un derecho fundamental protegido y garantizado por el Estado y los particulares, reglamentado en los diferentes estatutos normativos que persiguen, entre otros fines, la tutela efectiva de sus titulares y la garantía de su pleno ejercicio en las diversas órbitas jurisdiccionales: civiles [20], contencioso-administrativas, penales [21] y constitucionales e incluso en ámbitos de competencia no judiciales, es decir, en vía administrativa (o "gubernativa") y hasta en una vía *sui géneris* sancionatoria-administrativa desatada ante organismos independientes de los poderes públicos tradicionales v.gr. La Agencia de Protección de los Datos Española, o bien ante organismos gubernamentales dependientes de los Ministerios de Comercio, Industria y Turismo y al Ministerio de Hacienda y Crédito Público, como son las Superintendencias de Industria y Comercio y la Financiera, respectivamente en Colombia, a partir de la expedición de la Ley 1266 de 31 de Diciembre de 2008, para la pro-

---

(19) FARIÑAS M., Luis**. *El derecho a la intimidad*.** Ed. Trivium, S.A., Madrid, 1983, págs. 315 a 352.

(20) La moderna regulación del derecho a la intimidad en España, comienza con la expedición de la Ley Orgánica 1/1982, de 5 de mayo, que regula la protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Esta ley desarrolla el art. 18.1 CE, que garantiza tres derechos fundamentales, incluido la intimidad. Aunque se piensa que el derecho a la imagen no es más que una manifestación corporal de la intimidad [v.gr. El Caso Marks Vs. Joffa. El Tribunal de New York Aplicó los conceptos jurídicos de la "privacy" de Warren y Brandeis, en 1893 para darle razón al demandante cuando solicitaba tutela judicial por la publicación de su imagen (fotografía) en un periódico sin su consentimiento. Aquí se tuteló el "Right to privacy", por ser la imagen una emanación de la privacy], Texto completo en ***AA.VV. compendio de discos compactos aranzadi*.** Ed. Aranzadi, 1997.

(21) A partir de la Expedición del Código Penal de 1995, se erigió como bien jurídico constitucional autónomo, el derecho a la intimidad personal y familiar, que antes había sido protegido y tutelado con carácter de *ultima ratio* en España, como derecho constitucional sí, pero dentro del bien jurídico (que para muchos iuspenalistas resultaba, cuando menos, poco conveniente) denominado de la *Libertad y Seguridad de las personas.* Hoy, existe una dual protección punitiva del derecho a la intimidad: **a)** como bien jurídico autónomo, tutelado en el Libro II, Título X, Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad de domicilio (arts. 197 a 204); y **b)** como derecho fundamental bajo otros bienes jurídicos: Delitos contra la Constitución: De los delitos cometidos por los funcionarios públicos contra las garantías constitucionales (Tit. XXI. Cap. V). De los delitos cometidos por los funcionarios públicos contra la inviolabilidad domiciliaria y demás garantías de la intimidad (arts. 534 a 536).

tección sectorial de los datos financieros, pues el resto de datos personales que pueden ser objeto de sistematización y tratamiento informatizado jurisprudencialmente seguirán siendo protegidos por los organismos o dependencias públicas o privadas que vigilan, controlan, administran o son operadores de bancos de datos o ficheros, registros o archivos.

En el derecho colombiano el derecho fundamental a la Intimidad como bien jurídico tutelable, deviene de la connotación de derecho constitucional de interés particular, familiar y social, cuya valía se representa no sólo en la esfera de lo más íntimo del ser humano sino en las esferas exteriores donde la relevancia y efectos jurídicos materiales y morales afectan al ser individual, familiar y socialmente considerados, puesto que el uso, goce y disfrute del derecho por los cambios sociales, culturales, científicos y de todo orden, así como los avances de las nuevas tecnologías de la información y la comunicación –medios TIC— se ven altamente amenazados, vulnerados o transgredidos por tradicionales como modernos medios comisivos de infracciones o conductas punibles.

Las ciencias jurídicas, las ciencias de la comunicación y la Informática jurídica a través de diversas instituciones, figuras o mecanismos sustantivos o procesales propenden por la protección y defensa integral de los diversos derechos y libertades fundamentales, entre ellos el de la Intimidad y que pudieran estar involucrados en el tráfico de transgresiones o violaciones tradicionales o tecnológicas.

Por ello, haremos un breve comentario a aquellas áreas jurídicas de ***prima y ultima ratio*** que propenden por la protección individual o integral del derecho fundamental a la Intimidad.

2.1.1. En el ámbito Civil.

Preconstitucionalmente a 1991, la privacidad, la vida privada o la vida íntima que resultan ser esferas más internas del derecho a la intimidad, fueron reguladas en el Código Civil de 1887, hoy vigente con muchas reformas puntuales al mismo, en dos de sus muchas facetas, a saber: (i) “Las servidumbres de luz” y derechos y deberes de vecindad generada por la propiedad, posesión o tenencia de bienes inmuebles. También conocida como visión domiciliaria de la intimidad; y (ii) Daño moral subjetivo en la responsabilidad extracontractual: *dolor y dignidad humana.*

A la luz de la interpretación constitucional del artículo 16 de la fenecida Constitución de 1886, relativo a la protección de las personas por parte del Estado en su vida, honra y bienes se produjo prolija jurisprudencia y doctrina iuscivilista sobre protección a la intimidad de las personas, basado en el llamado derecho de vecindad: las servidumbres de luz (Artículos 931 y ss.); y b) el no menos delicado como fructífero tema de la “Responsabilidad extracontractual”, de su caracterización, y particularmente de uno de sus elementos más significativo: el daño (artículos 2341 y ss).

Las servidumbres luz, tiene “por objeto dar luz a un espacio cualquiera, cerrado y techado; pero no se dirige a darle vista sobre el predio vecino, esté cerrado o no. No se puede abrir ventana o tronera de ninguna clase en una pared medianera, sino *con el consentimiento del condueño.* El dueño de una pared no medianera puede abrirlas en ella en el número y de las dimensiones que quiera... La servidumbre de luz está sujeta a las siguientes condiciones: La ventana estará guarnecida de rejas de hierro, y una red de alambre, cuyas mallas tengan tres centímetros de abertura o menos y la parte inferior de la ventana distará del suelo de la ventana a que da luz, tres metros a lo menos”. Nace así en el derecho colombiano el concepto de la “intimidad domiciliaria” (“*My home is my castle*” frase férrea y esquemática vertida en el ensayo de Warren y Brandeis).

La intimidad del hogar se protege entre paredes, libres de miradas, comunicación de ruidos, transferencia de olores, etc. En el C.C., se plasma así: i) El que goza de la servidumbre de luz tendrá derecho a impedir que en el suelo vecino se levante una pared que quite la luz. Si la pared medianera llega a ser medianera, cesa la servidumbre legal de luz y sólo tiene cabida la voluntaria, determinada por mutuo consentimiento de ambos dueños; (art. 934 Código Civil--C.C.C--) y, ii) No se puede tener ventanas, balcones, miradores o azoteas, que den vista a las habitaciones, patios o corrales de un previo vecino, cerrado o no, a menos que intervenga una distancia de tres metros. (art.935 C.C.C). Por remisión expresa del art.913 del C.C., los trámites y procedimientos sobre estas servidumbres se traslado a la competencia civil de policía (Inspectores y Alcaldes). Por ello, los Códigos Departamentales y luego el Código Nacional asumieron estas competencias [22].

Respecto del derecho a reclamar *el Daño Moral* y su estructuración con base en la dignidad e intimidad de las personas, la Corte Suprema Colombiana, --C.S.J.-- Sala Civil, ha sostenido: (i) "La doctrina y la jurisprudencia han considerado necesario reservar este derecho (a reclamar el daño moral) a aquellas personas que, por sus estrechas vinculaciones de familia con la víctima del accidente, se hallan en situación de aflicción que les causa la pérdida del cónyuge daño a la corporeidad humana, va ínsita en este último" (Mar.5 de 1960), (ii) "...el llamado derecho moral subjetivo, por actuar sobre lo más íntimo del ser humano, sus sentimientos, no puede ser justipreciado con exactitud..." (Junio 11 de 1993), (iii) "... y los herederos podrían entonces reclamar resarcimiento, pero sólo por derecho propio, en la medida que demuestren quebranto de su individualidad y con él se hiciera presente su padecimiento afectivo o sentimental, habida consideración de los estrechos vínculos que los ataban al muerto (Octubre 20 de 1943), justificativos de dicha aflicción y consiguiente derecho (Abril 4 de 1968).

Con base en estos pronunciamientos se construyó la faceta de la intimidad de los sentimientos y estado de ánimo de las personas, en donde unos y otros tienen relevancia jurídica y digna de protección, reconocimiento y justipreciación económica.

En vigencia de la Constitución de 1991, la intimidad personal y familiar al consagrarse como derecho fundamental de protección inmediata y tutelable eficazmente a toda persona con base en los artículos 2, 15 y 86, constitucionales, se debe ratificar que las anteriores instituciones ius civilistas, aún siguen vigentes y produciendo textos jurisprudenciales más ajustados a la realidad social actual, las nuevas costumbres, los cambios sociales, económicos, jurídicos y tecnológicos que producen los medios TIC, y en fin, la sociedad moderna.

El daño moral ("*Pretium doloris*", precio del dolor) tiene entidad propia y no debe confundirse con el perjuicio de placer (o perjuicio por daño de vida de relación o "fisiológico"), aunque ambos sean especies del daño extrapatrimonial, ni con el daño material (daño emergente y lucro cesante), que es un daño eminentemente patrimonial (C.de E., Sec.III, Sentencia 11842 de Julio 19 de 2000).

Los daños morales se definen como aquellos perjuicios causados a los sentimientos de las personas, como a su honor, a su imagen o a sus afecciones legítimas, es decir a su vida espiritual. Además de las fuentes previstas en el artículo 2341 del C.C., de donde puede provenir el daño moral, se relacionan por la doctrina [23] diversas situaciones tales como: (i) la

---

(22) Vid. RIASCOS GOMEZ, L.O., ***La Constitucionalidad de la jurisdicción civil de policía.*** Tesis para optar el título de abogado, Facultad de Derecho, Univ.de Nariño, Pasto, 1983, pág. 33 y ss.

(23) Fernández Jiménez, Manuel**. La valoración pericial del daño moral.** *Director de la Unidad de Valoración del Daño Psicosocial-UVADAP.* **En:** http://www.graduados-sociales.com/

Violación de todo aquello que afecte a la vida íntima de la persona, (ii) Daños físicos y orgánicos y cualesquiera lesiones corporales que afecten a la salud física o psíquica de las personas, incluida la función libidinosa; (iii) Daños físicos y orgánicos y cualesquiera lesiones corporales que afecten a la estética o imagen corporal de las personas; (iv) Daños psíquicos y psicosociales que afecten a la salud psíquica de las personas, como el acoso laboral o sexual; (v) Cualquiera de los daños anteriores que afectan a la capacidad de goce, disfrute, confort u ocio; (vi) Atentados al honor, al prestigio o a la reputación personal; (vii) Atentados a los derechos fundamentales, como el de la libertad personal; (viii) Violación del domicilio u otras pertenencias materiales; (ix) Agresión, daño y muerte de las personas allegadas, tanto del ámbito familiar como del social o del laboral; y (x) Perjuicio juvenil y perjuicio social.

El artículo 90, de la Constitución de 1991, es la fuente de toda responsabilidad contractual y extracontractual del Estado, según lo ha ratificado los reiterados pronunciamientos del Consejo de Estado y la Corte Constitucional, pues hoy podemos hablar de una "cláusula general de responsabilidad patrimonial del Estado" (C-333-96), aplicable a todas las áreas del derecho y en todos aquellos casos en donde existe u "daño antijurídico" ocasionado por la acción u omisión de cualquier agente o autoridad estatal contra las personas o sus bienes. Todo daño material o moral debe ser indemnizado por el agente o la autoridad estatal, con lo cual si se producen atentados o vulneraciones de derechos fundamentales, como la intimidad, vida privada o el honor deberán ser resarcidos de conformidad con la cuantificación, valuación y determinación en sentencia judicial de los jueces de la República, previa demanda por la personas o personas legitimadas para incoar dicho reclamo y que en el caso de los daños morales serán aquellas personas afectadas en el "pretium doloris", los sentimientos y las aflicciones y conforme a variables dependientes del propio individuo, tales como: Su cultura o costumbres, su educación, sus creencias, su religión, su posición o estatus social y su nivel económico.

2.1.2. En el ámbito del derecho administrativo.

El derecho a la intimidad siempre ha estado presente dentro de la protección constitucional y legal que se da al derecho a la información. En efecto, existe suficiente e idónea legislación al respecto, pre y postconstitucional a 1991. La Constitución del 91, reconoció el derecho a la información (art.20 y 74) y el derecho de expresión (art. 20 y 73). "El derecho a la información no es solamente el derecho a informar, sino también el derecho a estar informado, informarse. De ahí la importancia del artículo 74 de la Constitución Nacional, que al consagrar el derecho de acceder a los documentos públicos hace posible el ejercicio del derecho a la información, y de esta manera los demás derechos fundamentales ligados al mismo", como el *habeas data*, la intimidad, el honor, honra, etc. (CC Sent 0-33, Feb. 8 de 1993).

El derecho a la información está reglamentado en las siguientes normas jurídicas: (i) Ley 4 de 1913, art.320 (Acceso a documentos públicos); (ii) Ley 74 de 1968, art. 14; (iii) Ley 16 de 1972, art. 13 y 14; (iv) En la Ley 57 de 1985, Julio 5, por la cual se ordenó la publicación y documentos oficiales, conocido en la doctrina como "Estatuto del Derecho a la Información". En éste Estatuto se regula, entre otros aspectos importantes: a) La información reservada: contenido, duración, rechazo --arts. 19 a 21--; b) Procedimiento para la consulta de documentos públicos (arts. 22 y ss); y c) Sanciones a los funcionarios que incumplan el contenido de la ley; (v) El Código Contencioso Administrativo (Decreto 01/1984 y Dec.2400/89).

En éste Código se reglamenta el derecho de petición (art.23 de la C.P.), así: En el Capítulo II, El derecho de petición en interés general: peticiones escritas y verbales, término para resolverlas, consecuencias de la desatención de las peticiones, desistimiento (arts.5 a 8). En

el Capítulo III, el Derecho de petición en interés particular: quiénes pueden hacerlas, requisitos especiales, peticiones incompletas, documentos a información insuficiente, desistimiento, citación de terceros, publicidad, costo de citaciones y publicaciones (arts. 9 a 16). En el Capítulo VI, sobre el derecho de petición de informaciones: derecho de información, información especial y particular, inaplicabilidad de excepciones, examen de documentos, plazos para decidir sanciones, notificación y recursos a las sanciones, costo de las copias (arts.17 a 24). En el Capítulo V, sobre el derecho de formulación de consultas: el derecho de petición incluye consultas, atención al público (arts. 25 a 26).

El derecho a la información por medios tecnológicos, informáticos y electromagnéticos se rige, por las siguientes normas:

1.- El Dec-ley.131 de 1976 de enero 26, por el cual se dictan normas sobre utilización de sistemas de información y de equipos de información y servicios de procesamiento de datos. Decreto reglamentado por los Dec.1160 de 1976, de junio 7, Res. 2145 de 1976, de Octubre 5.

2.- El Decreto-ley 2328 de 1982, de Agosto 2, por el cual se dictan normas sobre el servicio de transmisión o recepción de información codificada (datos) entre equipos informáticos, es decir, computadores u ordenadores y/o terminales en el territorio nacional.

3.- El Decreto-ley 148 de 1984, de Enero 24, por el cual se dictan normas sobre servicios de transmisión de información codificada (datos) para correspondencia pública.

4.- El Decreto-ley 260 de 1988, de Febrero 5, por el cual se reglamenta el "Sistema de Información automatizado en el sector Público" y las funciones asesoras, consultoras o gestionadoras del DANE (Departamento Nacional de Estadística). Reglamentado por el Decreto 1600 de 1988, por el que se integra una Misión de Ciencia y Tecnología y señala funciones al DANE.

5.- El Reglamento de la Asociación Bancaria y de entidades financieras de Colombia --ASOBANCARIA--, Marzo 23 de 1995, referente al manejo, procesamiento, almacenamiento, uso y transmisión de información económica financiera contenida en las bases de datos de ámbito del sistema del CIFIN --Central de Información de la Asobancaria-- de carácter particular. Las funciones de protección en vía administrativa ("mal llamada gubernativa", puesto que es viable ante cualquier rama del poder público y no en forma exclusiva y excluyente de la rama ejecutiva que es lo que sugiere el término "gubernativa"), del derecho de la información la adelanta el Ministerio Público, El Defensor del Pueblo y los Personeros Municipales, pues constituyen una especie de *L´Ombusdman del derecho a la información* o del Comisario para la protección de la información, como sucede en el derecho Canadiense.

6.- La Ley 527 de 1999, por la cual se reglamenta el acceso y uso de mensajes de datos, del comercio electrónico y las firmas digitales y se establecen las entidades de certificación y otras disposiciones. Así como los diversos decretos reglamentarios de dicha ley.

7.- Ley 962 de 2005, sobre la racionalización de trámites y procedimientos administrativos de las entidades y organismos del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos; y,

8.- Ley 1341 de 2009, por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones –TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.

El cuadro de protección y defensa del derecho fundamental de la intimidad, a partir del art. 18 CE, en España y el art.15 C.P., en Colombia, es tan amplio, como variado y regulado en forma pormenorizada en el ordenamiento jurídico vigente, a tal punto, que se conocen diversos niveles de protección: unos de tipo cautelar o preventivo, en vía administrativa; y otros, a nivel reparador e indemnizatorio en vías jurisdiccional civil y contencioso-administrativo; a nivel represivo o punitivo en el ámbito penal; y aún a nivel que podríamos llamar de protección *in integrum* en vía constitucional de *"recurso de amparo* [24], en España, o mediante la "acción *de tutela*"[25], en Colombia. Sin embargo, por ahora no son objeto de nuestra investigación, aunque vale la pena referenciarlos para entender el estado global actual de protección del derecho a la intimidad en España y en Colombia y poder dimensionar la particularidad específica de la protección de la intimidad, a través de la visión iusinformática.

Pese a ello, *Fariñas Matoni* [26] en 1983, consideraba que en España, la legislación para ese entonces vigente sobre el derecho a la intimidad era fragmentaria, anticuada, incompleta, asistemática, indirecta, esporádica e incidental, siendo deseable una nueva normativa actualizada y a la altura de los tiempos en que vivimos y que, sobre todo, vamos a vivir, y que contemple la cuestión: a), desde el punto de vista civil (el daño a la intimidad como modalidad especial del daño moral); b), desde el punto de vista penal, sancionando ciertos tipos de intromisiones; c), desde el punto de vista administrativo y preventivo, para evitar que se produzcan ciertas situaciones o se adquieran determinados instrumentos nocivos al derecho a la intimidad. Muy pronto las fundadas críticas del autor citado se ha visto reducidas a su mínima expresión, pues el marco de protección actual del derecho a la intimidad a la altura de

---

(24) El Tribunal Constitucional de España, tiene jurisdicción en todo el territorio español y ante éste se ejercita el recurso de amparo por la violación de los derechos y libertades fundamentales (incluido la intimidad), en los casos y formas que establezca la ley (arts. 53-2 y 161.1.a CE). LEY ORGANICA 3-10-1979.

(25) El art.86 regula este derecho fundamental de todas las personas para defender y garantizar todos los derechos y libertades públicas ante un juez de la República y por medio de proceso breve y sumario. Los Decretos 2591/1991, de 19 de Noviembre y 306 de 1992, desarrollaron la norma constitucional.

(26) El estudio del contenido de los derechos fundamentales, y en particular, en el de la intimidad es de tal variedad como de autores que lo exponen. En efecto, hay tesis con contenidos maximalistas (*Fariñas* y *Novoa Monreal*), otros prudentes (*Prosser* y *Frosini*) y otras tantos minimalistas, como la de *Westin* que resume los estadios de la privacy (Soledad, relaciones íntimas, anonimato y reserva), en "*el derecho de los individuos, grupos o instituciones de determinar por ellos mismos, cómo y cuanta información acerca de sí es comunicada a los otros".* Según Fariñas, el Contenido de la intimidad se divide en dos grandes ramas: 1. *En sí mismo, considerado fundamentalmente en cuanto a sí mismo*: 1. Con referencia a su pasado, que es o puede ser evocado en el presente contra su voluntad: a) derecho al olvido, b) derecho a mantener en secreto los recuerdos personales. 2. Con referencia a su presente, en el que es amenazado o atacado: 1) En su propio cuerpo: a)Tomas de sangre, orina, etc., b) Datos sobre su salud, c))Es el aborto una mera cuestión de la vida privada?, d) Narcoanálisis; 2) En aspectos no corporales: a) identidad, b) imagen, c) Datos personales, d) ser seguido u observado, e) objetos personales, f) placeres. 3. Con referencia a su futuro en cuanto planeado en el presente, potencialmente amenazado por ataques actuales: a) Descubrimiento de planes o proyectos del futuro. II. En sí mismo, considerado fundamentalmente respecto de los otros: 1. Los otros en cuanto colectivo: a) El Estado, en su doble papel de garante y amenaza de la intimidad; b) Personal (garante en cuanto emisor de normas protectoras, amenaza en cuanto compilador de otros datos personales, c) la sociedad y su interés en ser informada. 2. Los otros en cuanto personas concretas. 3. La intimidad ajena como límite y condicionante de la propia (el problema de la divulgación unilateral de un secreto compartido sin el consentimiento de la otra persona: a) la intimidad propia compartida: relaciones familiares (hogar, vida conyugal), relaciones cuasifamiliares (aventuras amorosas, amistades, comunicaciones y cartas), relaciones profesionales (vida profesional, secreto de los negocios); b) La intimidad propia amenazada por los otros: individuos concretos (parientes, vecinos, amigos, compañeros de trabajo, superiores, subordinados, extraños), sociedades, entidades o institucionales especializadas ad hoc (detectives, agencias de información o matrimoniales, otras entidades), El Estado (como administración y/o mediante sus funcionarios que cumplen o extralimitan sus funciones). **FARIÑAS M., Luis. *El derecho a la intimidad*.** Ed. Trivium, S.A., Madrid, 1983, págs. 355 a 367.

los Estados democráticos y consecuente con los adelantos tecnológicos TIC e informática.

2.1.3. En el ámbito punitivo.

En Colombia acorde con la tesis italianas sobre la clasificación del hecho o conducta punible, éste se divide en delitos y contravenciones y en consecuencia, el breve análisis de éste ámbito de protección de última ratio de la intimidad, se hará por un lado; en el plano contravencional, regulado en los Códigos de Policía Nacional, Distrital, Departamental y Municipal, según fuere el caso, mediante unos procedimientos policivo penales especiales para las contravenciones especiales y por autoridades administrativas con funciones cuasijurisdiccionales; y por otro, en un plano delictual, regulado en los Códigos Penal sustantivo y procesal vigentes, mediante un procedimiento jurisdiccional (investigación y juzgamiento) de carácter penal y por autoridades judiciales penales.

2.1.3.1. **En el plano contravencional**.

En Colombia, se protege a la "vida privada o íntima" bajo el bien jurídico tutelado de la integridad personal (Capítulo VIII, del Título IV, de las contravenciones especiales. Dec. 522 de 1971, que hace parte del Código Nacional de Policía –CNP-), de la siguiente forma: (i) "El que sin facultad legal averigüe hechos de la vida íntima o privada de otra persona, incurrirá en multa de cincuenta a cinco mil pesos. Si la conducta se realiza por medio de grabación, fotografía o cualquier otro mecanismo subrepticio, la multa se aumentará hasta en la mitad" (art. 46); (ii) "El que divulgue los hechos a que se refiere el artículo anterior, incurrirá en multa de cincuenta a cinco mil pesos. Si la divulgación se obtiene provecho personal, la multa se aumentará hasta en la mitad. En casos de reincidencia, la pena será de uno a seis meses de arresto" (art.47); (iii) "El que habiendo tenido conocimiento de un hecho de la vida ajena, la divulgue sin justa causa incurrirá en multa de cincuenta a dos mil pesos. Si divulga el hecho con obtención de provecho personal, la multa aumentará hasta en la mitad" (art. 48); y (iv) En los casos previstos por los tres artículos anteriores, la acción penal requiere querella de parte" (art. 49).

De esta forma en éste ámbito, constituyen contravenciones especiales, las siguientes: (i) Averiguar la vida íntima o privada (art. 46 CNP); (ii) La Divulgación de la vida privada o íntima. Dentro de esta contravención de indiscreción, tres tipos contravencionales agravados, así: a) Por divulgación, descubrimiento o indiscreción (Inciso 1º del artículo 47 Id); b) Por provecho personal (Inc. 2º Ibid); y c) Por conducta reincidente (Inc.3º Ibid); (iii) Indiscreción "sin justa causa" de la vida privada (Inciso 1º artículo 48º CNP) y dentro de éste una contravención agravada por provecho personal (Inciso 2º Ibid).

Igualmente se protege la "intimidad domiciliaria" bajo el bien jurídico tutelado del "Patrimonio", cuando se constituye como contravención especial, el "*que sea sorprendido dentro de habitación ajena, depósito, granero, caballeriza o cualquier otro lugar destinado a la guarda y custodia de animales u otros bienes, o dentro de tienda o almacén que no estén abiertos al público, y no justifique su presencia en tales lugares, incurrirá en arresto de seis a doce meses, si el hecho no constituye delito de violación de domicilio*".

"La Sanción se aumentará hasta en otro tanto, si el agente hubiere sido condenado dentro de los cinco años anteriores por delito contra la propiedad".

En este segundo inciso se plantea una contravención agravada de la "presencia injustificada en domicilio", cuando el agente hubiere sido condenado anteriormente (5 años) por delitos contra la propiedad. Se plantea la reincidencia como causal de agravación punitiva y por tanto no viola el principio del non bis in idem.

Las autoridades competentes son los Alcaldes y los Inspectores de Policía, en primera instancia; y los Gobernadores en segunda Instancia y de conformidad con el procedimiento especial previsto en los artículos 71 a 104 del CNP y en lo no previsto en éstos por las normas generales del Código sustantivo y procesal Penal y Código Procesal Civil, en lo que fueren pertinentes.

2.1.3.2. En el plano penal.

En el derogado Código Penal de 1980, se protegía a la *intimidad y el habeas* data bajo un bien jurídico tutelado diferente o bien como derecho fundamental implícito. En efecto, en el Título X, "*De los delitos contra la libertad individual y otras garantías*", Cap. V, "Delitos contra la violación de secretos y comunicaciones", así: 1. violación ilícita de comunicaciones (art. 288); 2. violación y empleo de documentos reservados públicos o privados (art. 289); 3. utilización ilícita de equipos transmisores o receptores (incluidos los electromagnéticos: informáticos y/o telemáticos); y, 4. interceptación ilícita de correspondencia oficial.

Los dos últimos previstos en el Dec. Ext. 2266 de 1991, arts. 16 y 18, respectivamente que fueron incorporados a la legislación penal especial en forma permanente.

Bajo otros bienes jurídicos tutelados: así:

A. *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*" (Art. 225 del Código Penal derogado, conc. Art. 274 C.P.P y 251 C.P.C.). Este concepto de documento electrónico se aplicará a los delitos: 1. Falsedad material de empleado oficial en documento público (art. 218); 2. Falsedad ideológica en documento público (art.219); 3. Falsedad material de particular en documento público (art. 220); 4. Falsedad en documento privado (art. 221); 5. Uso de documento público falso (art. 222); 6. Destrucción, supresión y ocultamiento de documento público (art. 223); y, 7. Destrucción, supresión y ocultamiento en documento privado (art. 224).

B. *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 (art. 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 Dec. 623 de 1993, conocido como "*Estatuto penal del sistema financiero colombiano*", concedía 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*" (arts. 105 y ss).

C. *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" (art.350). 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 (art.239 *in fine*). El derogado Código Penal del 80, amplió los medios comisivos al prever la obturación o rupturación de claves o "*password*" para acceder a la apropiación de bienes. 2. **Estafa** "*valiéndose de cualquier medio fraudulento..."* como el informático y/o telemático (art.256 *in fine*), configura lo que el C.P. Español denomina "*Estafa informática*" (art.248), 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*". **3. Daño agravado** cuando se comete en "*archivos*" (se entiende manuales o informatizados), art. 371.4.

D. *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 (Art.61 Constitucional).

En el Código Penal vigente (Ley 559 de 2000), reformado parcialmente y para nuestro objeto de investigación por la Ley 890 de 2004, se crea expresamente el bien jurídico tutelado de la intimidad bajo el Título III, de los delitos contra la libertad Individual y otras garantías, pero implícitamente se sigue protegiendo a la intimidad bajo otros bienes jurídicos tutelados tal como se hizo en el Código Penal de 1980 en los delitos contra la fe pública, el orden económico social, el patrimonio Económico y la propiedad intelectual, con algunas matizaciones puntuales que se harán más adelante.

En forma expresa la intimidad como bien jurídico tutelado se regula en el Título III, Capítulo VII, del Código Penal del 2000, junto a dos especies de la intimidad, como son la "reserva e interceptación de comunicaciones" que resultan inocuas, pues era suficiente que el legislador del 2000, hubiese estructurado el bien jurídico único, con la Intimidad, pero a no dudarlo, lo que pasó por la cabeza de los legisladores fue que sólo a través de la vulneración del derecho a reserva (o sigilo) en cualquier tipo de comunicaciones (tradicionales, informáticas, electrónicas o telemáticas), sean privadas u oficiales, era la única forma de transgredir o vulnerar la intimidad personal o familiar del ser humano. Aspecto éste que es, cuando menos incompleto dentro de ese amplio abanico de lo que constituye la Intimidad de las personas, como antes hemos visto en el pie de página número 26.

El legislador español de 1995, para evitar la reglamentación parcial de la intimidad como bien jurídico tutelado pluriofensivo creó dos grandes vertientes que cubren un mayor número de supuestos en los que se transgrede a la Intimidad, pues cada una de ellas a su vez, implican variados supuestos de la Intimidad (corpóreo, incorporal, de datos personales, de voz, imagen, de datos sensibles o del núcleo duro de la "privacy", de datos de personas físicas y jurídicas, de datos de personas en condiciones especiales o de menores de edad, de intimidad domiciliaria: morada y de lugares de trabajo, etc.). Esas dos vertientes son: (i) Delitos de Descubrimiento y de revelación de Secretos (Cap. I, Titulo X). Ese con tres tipos penales básicos y cuatro tipos penales agravados; y (ii) del Allanamiento de morada, domicilio de personas jurídicas y establecimientos abiertos al público. Ese con dos tipos penales básicos y dos tipos penales agravados.

El Código Penal de 2000, por su parte en los artículos 192 a 197, estructuró las siguientes conductas delictivas contra la Intimidad: (i) Violación ilícita de comunicaciones; (ii) Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas; (iii) Divulgación y empleo de documentos reservados; (iv) Acceso abusivo a

un sistema informático; (v) Violación ilícita de comunicaciones o correspondencia de carácter oficial; y (vi). Utilización ilícita de equipos transmisores o receptores.

La ley 1273 de 2009, que creó el bien jurídico tutelado de la "Información y los datos", trasladó el delito de acceso abusivo a un sistema informático, al Título VII Bis, artículo 269 A y le hizo algunos retoques de redacción, pero sobre todo aumentó la dosimetría penal aplicable a la figura penal, por considerar que las nuevas tecnologías de la información y la comunicación –TIC—vienen siendo cada día más penetrantes, invasoras de la información personal, familiar, mercantil, industrial, etc., contenidas en bases de datos o ficheros, archivos o registros informatizados o no.

Gran parte de los datos personales generales y sensibles afectan el derecho a la intimidad, al honor y el habeas data, por ello, hubiese sido más conveniente sin crear el bien jurídico de la "Información y los datos" (éstos últimos sobran, pues los datos son unidades de información escrita, virtual, auditiva, de video o cifrada y como tal la información es continente y los datos contenido), incluir varias de las conductas delictivas que aparecen bajo dicho bien jurídico en el bien jurídico de la intimidad haciendo claridad que se refiere a los datos personales generales o sensibles de la persona física exclusivamente, pues es cuestionable en nuestro Código como en el Código Penal Español de 1995, que se hable de delitos contra la intimidad de las personas jurídicas (artículo 201), pues éstas no tienen intimidad ya que es un derecho personalísimo de las personas naturales, las personas jurídicas a lo sumo tendrán un derecho a "Good Will", a no ser que se hable de la actividad delictiva contra la intimidad de las personas naturales que representan, dirigen o gerencian una empresa pública o privada.

De otro, lado el bien jurídico de la "Información", que hoy es más poder que nunca, debería estructurárselo como bien jurídico tutelado para toda aquella información que tenga un valor económico, tal como lo reclama Gutiérrez Francés [27] , en los delitos relativos al "mercado y a los consumidores", entre otros: (i) el apoderamiento de datos u objetos que se refieran al secreto (art. 278-1); (ii) Control audiovisual clandestino y control ilícito de señales de comunicación (art. 278-1 y 197-1); (iii) Tipo agravado de difusión, revelación o cesión a terceros de los secretos descubiertos (art. 278-2); (iv) Establece una "cláusula concursal", en el supuesto de realizar una conducta de apoderamiento o destrucción de los soportes informáticos. Concurso de delitos, pues con v.gr. el hurto simple o agravado; daños o sabotaje informático; (v) Delitos concernientes a los secretos de empresa (arts. 278 a 280 C.P. Español).

En este mismo sentido el legislador colombiano debió aprovechar la reforma al Código Penal, para estructurar debidamente el bien jurídico de la información con valor económico (empresarial, industrial, bursátil, bancaria, tributaria o financiera) bajo el bien jurídico tutelado de la Información con dicha connotación y valía diferente a la información o datos personales generales o sensibles del ser humano que perfectamente se podían incluir en el bien jurídico de la intimidad, como *ut supra* se dijo.

2.1.4. En el ámbito Internacional: Convenios, tratados y Declaraciones Universales.

Las normas de carácter continental y universal han regulado la protección estatal y de los mismos particulares de la vida privada o vida íntima, la privacidad o la intimidad. En efecto, ***la***

---

(27) Vid. GUTIERREZ FRANCES, María Luz. ***Delincuencia económica e informática en el nuevo código penal***.. En: Cuadernos de Derecho Judicial. Escuela Judicial. C.G.P.J. No. XI, Madrid, 1996. Además, ***Notas sobre la delincuencia informática: atentados contra la "información" como valor económico de empresa.*** En: Estudios de Derecho Penal Económico. Editores: Luis Zapatero y klaus Tiedemman. Ed. Univ. de Castilla-La Mancha. Tarancon (Cuenca). 1994, pág. 183 a 208.

Declaración Universal de los Derechos del Hombre, de 10 de Diciembre de 1948, adoptada y promulgada por la Asamblea General de las Naciones Unidas en su Resolución 217A (III), en la reunión celebrada en la ciudad de Bogotá, en declara expresamente garantiza la "*vida privada*" como derecho objeto-sujeto de protección estatal por parte de los Estados Miembros (entre ellos, España y Colombia). El artículo 12 sostiene: "*Nadie será objeto de injerencias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias y ataque*".

Las injerencias de toda persona física o jurídica, pública o privada en la intimidad de otro, se extiende a la de la familia, a su domicilio y a su correspondencia. Se confirma así, la protección no sólo del concepto de intimidad personal sino de la institución socio-jurídica de la familia (o intimidad familiar), la intimidad primigeniamente epistolar, es decir, la correspondencia escrita (pública o privada) y se refuerza expresamente aquello que Warren y Brandeis, citando a los ingleses, denominaron *My home is my* castle (la intimidad domiciliaria). Visiones conceptuales actuales de la intimidad estas dos últimas (a través de la inviolabilidad de la correspondencia y del domicilio), que preceden al concepto mismo de *the right to privacy,* tanto en la legislación, como en las diversas Constituciones del mundo [28].

De Cupis, tomando los elementos de conceptualización de la *privacy* inmersos en el ensayo Warren y Brandeis y la ampliación institucional vertida por la Declaración Universal, define la intimidad "como aquel modo de ser de la persona que consiste en la exclusión del conocimiento ajeno de cuanto hace referencia a la propia persona o también como la necesidad consistente en la exigencia de aislamiento moral, de no comunicación externa de cuanto concierne a persona individual" [29]. Toma el derecho de la intimidad, sólo como el derecho a salvaguardar la ajenidad de la persona (*the right to let alone*), como sujeto individualmente considerado (física como moralmente).

En igual sentido, los diversos Tratados y Acuerdos Internacionales *sobre Derechos Humanos* que siguieron a dicha declaratoria proclamaban expresamente la protección y tutela estatal como la de los mismos particulares del derecho a la intimidad personal, familiar y del menor.

El Convenio para la protección de los Derechos Humanos y las libertades fundamentales de Roma: El derecho a la intimidad personal y familiar es un *derecho autónomo pero no absoluto*. Los Estados miembros del Consejo de Europa, de aquélla época, tras la Declaratoria Universal de los Derechos Humanos, creyeron conveniente asegurar el reconocimiento y aplicación efectivos de los derechos proclamas por la Asamblea General de las Naciones Unidas el 10 de Diciembre de 1948, a fin de afianzar las bases mismas de la justicia y de la paz en el mundo, y cuyo mantenimiento reposaba esencialmente, de una parte, en un régimen político verdaderamente democrático, y, de otra, en una concepción y respeto comunes de los derechos humanos. Para fortalecer hacia el futuro estos ideales, el Consejo de Europa, acordó la emisión del Convenio de protección de Derechos Humanos y libertades fundamentales, actualmente conocido como *Convenio de Roma, 1950*

---

(28) En la Constitución de los EE.UU: La IV Enmienda de 1787 (Inviolabilidad de domicilio como de las personas, papeles y efectos); La Constitución de Bélgica de 7 de Febrero de 1831 (El secreto de correspondencia es inviolable); La Constitución Argentina de 1 de mayo de 1853 (Inviolabilidad de domicilio); La Constituciones de España de 1869, 1873 y 1876 (Inviolabilidad de correspondencia); y, La Constitución de Colombia de 1886 y 1991 (Inviolabilidad de correspondencia y domicilio)

(29) Citado por LOPEZ DIAZ, E., ***Derecho al honor y el derecho a la intimidad****. Jurisprudencia y Doctrina.* Ed. Dykinson, Madrid, 1996, pág. 197.

y el cual tardíamente fue ratificado por España, mediante instrumento de 26 de Octubre de 1979.

En esencia, el contenido del Convenio es similar a la Declaración de Derechos Humanos, con diferencias puntuales, pero tiene la virtualidad de ser un instrumento jurídico con efectos vinculantes entre los Estados miembros del Consejo de Europa, hoy de la Unión Europea (U). Quizá por ello, actualmente en España, los Tribunales Judiciales en las áreas penal, civil, social ("laborales"), administrativas, y sobre todo constitucional (TC. Sentencias: Jul. 14/1981; Nov. 15/1982; Jun.6/1994; Feb.23/95; Oct. 25/1995; Dic.11 de 1995; Mar.3/1996; Jul.9/1996; Mar. 26./1996; Nov. 5/1996), basan sus pronunciamientos en el Convenio de Roma (art.10-2 CE), puesto que los Convenios ratificados por España, tienen efectos jurídicos vinculantes para los poderes públicos y son un factor de interpretación de los derechos humanos (STC Núm. 254/1993, de 20 de Jul.), cuando ingresan al ordenamiento jurídico interno previa publicación en el Boletín Oficial del Estado (BOE art.96-1 CE).

El Convenio, reconoce que *toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás* (art.8).

El Convenio protege el derecho a la intimidad de las personas y de la familia (llámese familia "legítima e ilegítima", según el TEDH --Tribunal Europeo de Derechos Humanos-- desde la Sentencia de 13 Jun. 1979 --caso *Marcky*--, en el cual se declaró que *el artículo 8 no distingue entre familia legítima e ilegítima+ v.gr. en el caso *Johnston* --S TEDH 18 Dic. 1986-, tuteló los derechos de una unión conyugal de hecho de más de quince años de convivencia afectiva. Cfr. STC. 184. Nov. 15 de 1990).

De otro lado, establece que el derecho a la intimidad siendo un derecho fundamental y autónomo no es absoluto, lo cual quiere decir, que puede ser limitado o restringido su ejercicio, jamás hacerlo nugatorio, siempre que se den unas causales expresamente previstas. El Convenio, por tanto, proscribe toda injerencia al derecho a la intimidad, salvo que esté prevista: a) en la ley, b) sea necesaria para la seguridad nacional o pública, c) el bienestar económico del país, d) la defensa del orden y la prevención del delito, e) la protección de la salud o de la moral (STC Nov.15/1982, "la moral pública como límite del derecho de expresión, art.20-4 CE"); y, f) la protección de los derechos y las libertades de los demás. Estas excepciones a la injerencia e intromisión en el derecho a la intimidad, plantea actualmente uno de los aspectos constitucionales de mayor interés doctrinal y jurisprudencial, cual es el de los límites a los derechos y libertades fundamentales, al reconocérsele que éstos no son derechos absolutos en una sociedad democrática y pluralista y tenerse en cuenta que no puede afectarse el contenido esencial (o del núcleo) de los mismos, que los conduzca a desvirturarlo, hacer imposible su ejercicio, o peor aún a eliminarlos. En España, para guardar ese equilibrio del contenido esencial y la aplicabilidad de los límites de los derechos, se acude a la interpretación de los arts. 53-1 y 10 CE.

El "*Pacto Internacional de Derechos Económicos, Sociales y Culturales*". Fue adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General de las Naciones Unidas en la Resolución 2200a (XI) de 16 de diciembre de 1966. En Colombia se incorporó al ordenamiento jurídico interno mediante la Ley 74 de 1968.

En este documento de la ONU se reconoce el fundamento socio-jurídico y los elementos del derecho a la intimidad, así como la obligación del Estado y los mismos particulares de su respeto y protección.

En efecto, se reconocen los elementos integrales como el fundamento del derecho a la intimidad, paradójicamente sin hacer mención explícita a la vida privada. En efecto, se sostiene que los derechos humanos reconocidos en la Declaración Universal de 1948; entre ellos, la intimidad, se desprenden de "la dignidad inherente a la persona humana", por lo tanto, es obligación de los Estados "promover el respeto universal y efectivo" de los mismos, y "comprendiendo que el individuo, por tener deberes respecto de otros individuos y de la comunidad a la que pertenece, está obligado a procurar la vigencia yobservancia de" aquéllos derechos (Consideraciones del Pacto).

Los elementos caracterizadores del derecho a la intimidad personal y familiar se hallan tras el reconocimiento de lo siguiente: a) el derecho de toda persona a un nivel adecuado para sí y su familia y basado en el libre consentimiento (art.11-1); b) que la familia es el elemento natural y fundamental de la sociedad, a la que se debe prodigar la más amplia protección y asistencia posible (art.10); c) el derecho de toda persona al disfrute del más alto nivel posible de salud física y mental (art.12), d) que la educación se orienta al pleno desarrollo de la personalidad humana y del sentido de su dignidad (art.13); y, e) el derecho a la vida cultural y al progreso científico.

El Pacto Internacional de Derechos Civiles y políticos de 16 de diciembre de 1966, o también, "Pacto de New York". El articulado fue adoptado y abierto a firma, ratificación y adhesión por la Asamblea General por medio de la Resolución 2200A (XXI). En Colombia se incorporó al ordenamiento jurídico interno mediante la Ley 74 de 1968.

El art. 17 de este documento normativo ONU al reconoce expresamente el derecho a la vida privada, lo hace mediante un contenido textual "casi idéntico al art. 12 de la Declaración Universal de Derechos del Hombre". Sin embargo, el marco jurídico en el que está inmerso es totalmente diferente, porque como veremos junto al derecho de la intimidad se correlacionan otros derechos que influyen directa o indirectamente en su constitución. Además el Pacto Internacional de derechos económicos, sociales y culturales, sirvió de fundamento para el reconocimiento expreso del derecho a la intimidad y otros derechos humanos considerados fundamentales como la vida.

El artículo 17, sostiene: *1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación; y, 2. Toda persona tiene derecho a la protección de la ley contra injerencias o esos ataques.*

En efecto, todo Estado debe respetar y garantizar a todos los individuos que se encuentren en su territorio y estén sujetos a su jurisdicción los derechos y libertades fundamentales, sin *distinción alguna de raza, color, sexo, idioma, religión, opinión política o de otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición social* (art.2). Aspectos que constituyen la causa y razón de ser de todo derecho humano (en particular, del principio-derecho de igualdad, art.28) y algunos motivos (raza, color, sexo, idioma, religión u origen social) están excluidos de toda causal de excepción y aún en circunstancias excepcionales del Estado (art.4).

El derecho a la intimidad personal y familiar, como derecho fundamental inherente a la persona humana, cuya esencia hunde sus raíces en la dignidad, en el libre desarrollo de la personalidad, igualdad y libertad en una sociedad civil y pluralista se plasma en el Pacto, así:

a) En el principio de interdicción en la interpretación que desconoce o reconoce derechos a un grupo o individuo que pretenda quebrantar derechos y libertades de la persona (art.5-1); b) El derecho a la vida es inherente a la persona humana (art.6-1); c) Está proscrita toda forma de tortura, pena o trato cruel, inhumano o degradante. *Nadie será sometido, sin su consentimiento a experimentos médicos o científicos* (art.7); d) Todo ser humano tiene derecho al reconocimiento de su personalidad jurídica (art.16); e) Toda persona tiene derecho a la libertad de pensamiento, de conciencia y religión (art. 18); f) La familia es el elemento natural y fundamental de la sociedad (art.23); y, g) Todo niño tiene derecho, sin discriminación alguna, a la protección de su familia como de la sociedad y el Estado (art.24).

Los motivos más comunes y corrientes de colisión del derecho a la intimidad, con otros derechos como los derechos de opinión, expresión e información, por ejemplo, se patentizan en el ejercicio recíproco de éstos y aquél, y por ello el Pacto reconoce que nadie podrá ser molestado a causa de sus opiniones. Toda persona tiene derecho a la libertad de expresión; *este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole*, sin consideración de fronteras (sean orales, escritas, impresas o artísticas, etc). Este derecho sólo podrá ser restringido expresamente por ley y cuando sea necesario para: 1) Asegurar el respeto a los derechos o a la reputación de los demás, y 2) la protección de la seguridad nacional, el orden público o la salud o la moral públicas (art.19).

Los pronunciamientos de los Tribunales Judiciales sobre "*las injerencias ilegales*" al derecho de la intimidad, tanto colombianos [30] como españoles, han acudido reiteradamente al texto del art. 17 del Pacto de New York, para fundamentar sus pronunciamientos, en aplicación de los tratados internacionales como una de las fuentes del derecho y/o en el factor de hermenéutica interpretativa de los derechos y libertades fundamentales (art. 93 Constitución colombiana y 10-2 CE, respectivamente).

La Convención Americana Sobre Derechos Humanos o Pacto de San José de Costa Rica. La Convención se suscribió el 22 de noviembre de 1969, en la conferencia especializada interamericana de Derechos Humanos. En Colombia se aprobó mediante Ley 16 de 1972.

En parecidos términos y contenidos a los anteriores textos normativos internacionales el Pacto de San José, reitera la calidad de derecho inherente a la calidad de la persona humana el que llama "derecho al respeto de su honra y al reconocimiento de su dignidad". El Pacto quiere profundizar más en la protección del derecho a la intimidad (que lo sigue llamando vida privada, como coletilla inseparable de la intimidad) y lo hace yendo a la referencia de dos aspectos del núcleo del derecho como son honra y la dignidad humanas (art. 11). En tal virtud, *nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. Toda persona tiene derecho a la protección de la ley contra injerencias o esos ataques.*

De la esencia del derecho a la intimidad es el derecho que el Pacto denomina "*Derecho a la integridad física. 5-1. Toda persona tiene derecho a la que se respete su integridad física, psíquica y moral*". En la actualidad, se ha extendido este aspecto al estudio y análisis de la *visión corporal de la intimidad*.

---

(30) Así se ha hecho en los pronunciamientos de la Corte Constitucional Colombiana sobre derechos fundamentales, en particular del derecho a la intimidad, habeas data, honra, libre desarrollo de la personalidad, a partir de la Constitución de 1991.v.gr. Sentencia T-444, Julio 7 de 1992, T-022 de 1993, Enero 29, T-413/93, de 29 de Sep.,T-454 de 1995, T-696 de 1996, Dic. 5 y T-552 de 1997, de Oct. 30

El Convenio de Roma desde 1950, siguiendo en esencia los parámetros de la Declaración Universal de Derechos Humanos, tiene especial relevancia en este Estatuto normativo internacional, por cuanto, se sostiene expresamente "la protección de la familia" y sus miembros (en especial del niño art.11), como elemento natural y fundamental de la sociedad, por parte de los particulares y el Estado (art.17).

3. LA INTIMIDAD PERSONAL Y FAMILIAR EN LA JURISPRUDENCIA DE LA CORTE CONSTITUCIONAL: LA TUTELA COMO VIA DE PROTECCION Y DEFENSA

El derecho a la intimidad, como un derecho de toda persona ha sido elevado a rango constitucional y categoría de fundamental por la mayoría de Constituciones del mundo, incluida la Constitución Colombiana de 1991, tal como se prevé en el artículo 15, pero fundido a otros derechos constitucionales como el habeas Data y el "buen nombre", la inviolabilidad de las comunicaciones y la restricción al acceso de documentos privados por parte del Estado.

La Corte Constitucional en el transcurso de su labor de intérprete, guarda y vigilante de la Constitución, paulatinamente iría dando autonomía a cada uno de ellos, pero curiosamente las sentencias de tutela sobre la reserva, confidencialidad y disponibilidad de los datos personales mayoritariamente de carácter económico o bancario, serían los que posibilitaron dicha labor, no sin antes pasar por tres etapas jurisprudenciales: (i) fundición de los derechos de habeas Data e Intimidad para explicar la vulneración de éste último a través del desconocimiento de las facultades del derecho de habeas Data (conocer, almacenar, registrar, rectificar y actualizar la información) por los particulares o por el Estado mismo, al conformar bancos de datos sin el lleno de los requisitos de ley o medidas efectivas de seguridad informática; (ii) Deslinde de los derechos de Habeas Data, buen nombre e Intimidad, siguiendo los pasos del Tribunal Supremo Español en la sentencia 254 de 1993, sobre reserva potenciada de datos personales sensibles en ficheros o bancos de datos públicas, y crear jurisprudencialmente el "derecho a la autodeterminación informática o informativa" o también conocida "Libertad informática"; (iii) La autonomía del Habeas Data, la Intimidad y el buen nombre, a pesar de estar refundidos en un mismo artículo y diferentes incisos (Intimidad y habeas Data) e inclusive en un mismo inciso (Intimidad y buen nombre). Estas tres etapas, las comentaremos con más amplitud *ut infra*.

En la Constitución Española de 1978, en el artículo 18, el derecho a la intimidad, aparece redactado junto al derecho al honor, el derecho a la "propia imagen", la inviolabilidad de domicilio, el derecho al secreto o sigilo en las comunicaciones y el derecho a la limitación de la informática para garantizar el honor y la intimidad, que el Tribunal Supremo Español, en varios pronunciamientos denomina: "derecho a la autodeterminación informática o Habeas Data". El Tribunal Supremo a través de sus pronunciamientos reiterados sobre los datos personales contenidos en bases de datos o ficheros públicos o privados, construyó una derecho de "libertad informática o informativa" el cual sólo es posible entendiendo a la intimidad de la información que le concierne a una persona, cual sea el medio en el que se contenga (informático, electrónico o telemático, o manual), protegida por medios jurídicos efectivos y mecanismos informáticos de seguridad.

Por su parte, la Constitución Portuguesa de 1976, en el artículo 26.1, en artículos separados el derecho a la inviolabilidad de la integridad moral y física (art. 26-1); el derecho a la reserva de la intimidad privada y familiar (art.33-1); el establecimiento de garantías efectivas contra la utilización abusiva, o contraria a la dignidad humana, de informaciones relativas a las personas y a las familias (art.33-2); el derecho a la inviolabilidad del domicilio y el secreto de la correspondencia y demás medios de comunicación privada (artículo 34-1); Queda prohibida toda injerencia de las autoridades públicas en la correspondencia y en las telecomunicaciones, salvo los casos previstos en la ley en materia de enjuiciamiento (artículo

34-4); derecho a tomar conocimiento de la información que le concierne, y en su caso, a la rectificación y actualización de la misma (artículo 35-1). Esto se conoce con facultades básicas del derecho de "Habeas Data"; No se podrá utilizar la informática para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, salvo cuando se trate de la elaboración de datos no identificables para fines estadísticos (artículo 35-2); Se prohíbe atribuir un numero nacional único a los ciudadanos (artículo 35-3).

La Constitución Portuguesa con dedicación y excelente técnica legislativa relaciona los diversos derechos y deberes constitucionales que tiene la persona y cómo el Estado debe garantizarlos efectivamente. Le corresponde al operador o investigador jurídico hallar los correspondientes entronques que unos y otros derechos y deberes tienen o solucionar los posibles conflictos que éstos tuvieren en la aplicación a los casos o circunstancias concretas. Así por ejemplo, cuando se habla de la intimidad en relación con el derecho de habeas data es evidente que los datos de la persona como unidades de información (audio, video, escritos reales o virtuales, cifradas o binarias) que tienen reserva general o potenciada (datos sensibles o del núcleo duro de la "privacy") deben ser estudiados con la aplicación sistémica de los artículos 26.1, 33-1, 33-2, 34-1, 34-4 y 35-1 y 2.

Ahora veamos las etapas jurisprudenciales sobre el derecho a la intimidad en Colombia.

3.1. Primera Etapa jurisprudencial. A partir de la Constitución de 1991, la Corte Constitucional es la máxima autoridad judicial de carácter constitucional que tiene la guarda de la integridad y supremacía de la Constitución y revisar como Tribunal de última instancia, las acciones de tutela que se presenten por toda persona que crea se le han amenazado o vulnerado sus derechos constitucionales, a través de un proceso constitucional breve y sumario (artículos 241-9 y 86 C.N.).

En esta primera etapa el derecho a la intimidad sólo tiene explicación cuando se amenazan o desconocen datos personales de carácter económico y sobre todo de índole bancario, pues el "habeas Data" el que garantiza y protege la Intimidad de las personas, o bien cuando la intimidad entra en conflicto o en complementariedad con derechos y libertades constitucionales como el de información, libre expresión, pensamiento y libre desarrollo de la personalidad, o bien se entiende la intimidad, la honra y el buen nombre como atributos de la dignidad y el respeto mutuos de la persona humana.

En efecto, en la Sentencia T-022-1993, la Corte sostuvo: *"En la recolección y circulación de datos económicos personales se halla casi inevitablemente involucrado un problema de intimidad. Siendo esto así, es claro también que se configuran los presupuestos legales para la procedencia de la acción de tutela. Porque no solo entraña directamente la vulneración o amenaza de la intimidad del titular, sino porque la entidad que administra el banco de datos económicos personales es una organización frente a la cual su titular se encuentra la mayoría de las veces -especialmente en aquellos países que como Colombia carecen de una legislación específica que regule la circulación de datos personales- en condiciones de manifiesta indefensión".*

En la sentencia anterior, también podemos leer: "*Tanto el habeas data como la intimidad encuentran su razón de ser y su fundamento último en el ámbito de autodeterminación y libertad que el ordenamiento jurídico reconoce al sujeto como condición indispensable para el libre desarrollo de su personalidad y en homenaje justiciero a su dignidad. Dentro de ese refugio jurídicamente amurallado que lo protege, el sujeto puede actuar como a bien lo tenga. De ahí que las divulgaciones o investigaciones que penetren tal muro sólo podrán ocurrir por voluntad o aquiescencia del sujeto o cuando un verdadero interés general legitime la injerencia".*

En la Sentencia T-176-1995, la Corte manifiesta: "*Para que exista una vulneración del derecho al habeas data, la información contenida en el archivo debe haber sido recogida de manera ilegal, sin el consentimiento del titular del dato (i), ser errónea (ii) o recaer sobre aspectos íntimos de la vida de su titular no susceptibles de ser conocidos públicamente (iii)".* Y agrega, "*Se han establecido, de manera provisional, unos límites a la permanencia del dato en los archivos, en el entendido de que la reglamentación del habeas data es facultad del legislador. A juicio de esta Corporación, la mala conducta comercial pasada no debe ser mantenida en el archivo a perpetuidad. Sin embargo, un límite de los datos en el tiempo debe armonizarse con la necesidad de información sobre el comportamiento comercial que permita a las instituciones financieras calcular sus riesgos".*

En la sentencia T-414-1992, Julio 16, en caso de conflicto entre la intimidad y el derecho de la información, manifestó: la "prevalencia del derecho a la intimidad sobre el derecho a la información, es consecuencia necesaria de la consagración de la dignidad humana como principio fundamental y valor esencial… (en el) Estado social de derecho en que se ha transformado hoy Colombia…La intimidad es… (un) elemento esencial de la personalidad y como tal tiene una conexión inescindible con la dignidad humana…Solo puede ser objeto de limitaciones en guarda de un verdadero interés general que responda a los presupuestos establecidos en el artículo 1º de la Constitución…".

En la sentencia T-261-1995, la Corte considera que "*la protección constitucional de la intimidad no puede ampliarse indefinidamente hasta el extremo de considerar que todo dato personal sea a la vez íntimo…De los datos personales –concepto genérico—hace parte todas las informaciones que atañen a la persona y, por lo tanto, pueden ser, junto con las estrictamente reservadas, las referentes a aspectos que relacionan a la persona con la sociedad y que, por tanto son públicas…De tal modo, hay datos personales que específicamente son íntimos y gozan, en consecuencia, de la garantía constitucional en cuanto tocan con un derecho fundamental e inalienable de la persona y de su familia, al paso que otros, no obstante ser personales, carecen del calificativo de privados, toda vez que no únicamente interesan al individuo y al círculo cerrado de su parentela, sino que, en mayor o menor medida, según la materia de que se trate, tienen importancia para grupos humanos más amplios (colegio, universidad, empresa) e inclusive para la generalidad de los asociados, evento en el cual son públicos, si ello es así, están cobijados por otro derecho, también de rango constitucional, como es el derecho a la información (art. 20 C.N.)…". Agrega: "la dirección de un individuo…no puede mantenerse en secreto… (sin embargo), no puede desconocerse que algunas personas, por razón del cargo…o especiales riesgos para su vida o integridad pueden necesitar que su dirección y teléfono permanezcan en reserva, y en tales circunstancias, tiene derecho a ella…"*

En Sentencia de Unificación, SU-056-1995 la Corte sostuvo: "*El derecho al buen nombre es esencialmente un derecho de valor ("reputación que acerca de una persona tienen los demás miembros de la sociedad") porque se construye por el merecimiento de la aceptación social, esto es, gira alrededor de la conducta que observe la persona en su desempeño dentro de la sociedad. La persona es juzgada por la sociedad que la rodea, la cual evalúa su comportamiento y sus actuaciones de acuerdo con unos patrones de admisión de conductas en el medio social y al calificar aquellos reconoce su proceder honesto y correcto. Por lo tanto, no es posible reclamar la protección al buen nombre cuando el comportamiento de la persona no le permite a los asociados considerarla como digna o acreedora de un buen concepto o estimación."* –Paréntesis fuera de texto—

3.2. Segunda Etapa jurisprudencial. Basados en el principio de derecho universal que ningún derecho fundamental es absoluto, porque puede estar limitado por el derecho de los demás, por otros derechos y deberes y libertades públicas, o por razones de interés social o

comunitario, el derecho a la intimidad comienza a experimentar los límites y autolímites ejercidos por otros derechos y libertades públicas en beneficio mutuo y con el propósito de ir deslindando el verdadero entendimiento de cada derecho fundamental de la persona. En este sentido la Corte tiene varios pronunciamientos, en los que deslinda el derecho a la intimidad y el habeas Data y comienza a darles identidad y alcances en su protección y vulnerabilidad por parte de los particulares y el Estado. Todo a raíz de los variadas sentencias de tutela y las de unificación de jurisprudencia emitidas por la Corte, sobre los datos personales financieros, especialmente los correspondientes a las obligaciones para con las instituciones de crédito que tiene una persona y su forma de cumplirlas, "*realmente no pertenece al ámbito de su intimidad sino que -por el contrario- se trata de una situación que resulta de interés de los demás asociados, toda vez que se encuentran de por medio, además de sus recursos económicos, las expectativas de otros potenciales acreedores*" (T-552-1995).

En mentada Sentencia, se sostiene que *"El derecho a la intimidad implica la facultad de exigir de los demás el respeto de un ámbito exclusivo que incumbe solamente al individuo, que es resguardo de sus posesiones privadas, de sus propios gustos y de aquellas conductas o actitudes personalísimas que no está dispuesto a exhibir, y en el que no caben legítimamente las intromisiones externas. Algunos tratadistas han definido este derecho como el "control sobre la información que nos concierne"; otros, como el "control sobre cuándo y quién puede percibir diferentes aspectos de nuestra persona". La Corte Constitucional, por su parte, ha definido el núcleo esencial del derecho fundamental a la intimidad como "el espacio intangible, inmune a las intromisiones externas, del que se deduce un derecho a no ser forzado a escuchar o a ser lo que no desea escuchar o ver, así como un derecho a no ser escuchado o visto cuando no se desea ser escuchado o visto."*

"El derecho a la intimidad es un derecho disponible. Ciertas personas, según su criterio, pueden hacer públicas conductas que otros optarían por mantener reservadas. Así mismo, en el desarrollo de la vida corriente, las personas se ven impelidas a sacrificar parte de su intimidad como consecuencia de las relaciones interpersonales que las involucran. En otros casos, son razones de orden social o de interés general o, incluso, de concurrencia con otros derechos como el de la libertad de información o expresión, las que imponen sacrificios a la intimidad personal…" Y agrega: **"***A pesar de que en determinadas circunstancias el derecho a la intimidad no es absoluto, las personas conservan la facultad de exigir la veracidad de la información que hacen pública y del manejo correcto y honesto de la misma. Este derecho, el de poder exigir el adecuado manejo de la información que el individuo decide exhibir a los otros, es una derivación directa del derecho a la intimidad, que se ha denominado como el derecho a la "autodeterminación informativa"* **[31]** *.*

---

(31) Toma como punto de partida a no dudarlo, para comenzar a hablar del derecho a "autodeterminación informativa", los argumentos fáctico-jurídicos vertidos en la Sentencia 254 de 1993 del Tribunal Constitucional Español, que luego de analizar que los datos personales insertos en bases de datos de carácter público, sin el consentimiento del titular en su sistematización o procesamiento, vulneran el derecho a la intimidad y la "libertad informática", prevista en el artículo 18-1 y 18-4 de la CE. Este fallo, a su vez retomó el derecho de "*autodeterminación informativa* o informática" de la Sentencia de 1983 emanada del Tribunal Federal Alemán, relativa a la inconstitucionalidad de la "Ley de Censo" de 1982, por incluirse en la ley demasiados datos de la persona humana innecesarios para la labor de las autoridades competentes del censo, pero que revelaban la posición económica, patrimonial, ideológica, entre otras sensibles de la persona censada, por esta razón el Tribunal sostuvo que la Ley vulneraba entre otros derechos: el derecho del libre desarrollo y la autonomía de la persona y el de información. Como se ve la fuentes de vulneración constitucional en los tres Tribunales es diferente, aunque se llegue a la misma conclusión: la enunciación de un "nuevo" derecho jurisprudencial, como es el de la autodeterminación informática o informativa o "libertad informática", como se adicionó por el Tribunal Constitucional Español, al interpretar la limitación de la informática frente a los demás derechos y libertades públicas (18-4 de la CE).

Más adelante deja claro el deslinde de los derechos de habeas data y el de Intimidad, así: “El derecho al habeas data es, entonces, un derecho claramente diferenciado del derecho a la intimidad, cuyo núcleo esencial está integrado por el derecho a la autodeterminación informativa que implica, como lo reconoce el artículo 15 de la Carta Fundamental, la facultad que tienen todas las personas de "*conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas",* y si se pide actualizar o rectificar la información es por ésta ha sido recopilada no siendo veraz, actual o completa, o porque es errónea o no se ajuste a la verdad.

3.3. Tercera Etapa jurisprudencial.

En la Sentencia T-729-2002, la Corte Constitucional analiza los datos personales de un ciudadano colombiano, que sin su consentimiento han sido tratados informáticamente y consiguientemente almacenados, registrados y puestos en circulación en la Internet con acceso público. Las bases de datos así conformadas se realizaron por el Departamento Administrativo del Catastro de Bogotá y la Superintendencia Nacional de Salud, y los datos personales a los que pueden acceder vía internet, por cualquier persona con solo digitar el número de la cédula de un ciudadano, se pueden obtener información patrimonial concreta con muchos elementos precisos con número de predios, extensiones y valor predial, la que se refiere al Departamento de Castro; y otros datos personales no sólo que se refieren a la afiliación de la persona al sistema de seguridad social en Salud, sino a datos personales colaterales que reflejan información adicional sólo necesaria y pertinente para el afiliado o usuario de la base, pero no para cualquiera otra a quien no le conciernen dichos datos, pero que sí pueden ser utilizados por terceros con fines no legítimos o legales.

Por lo anterior, la Corte concluye que en estos casos se vulnera el derecho a la “autodeterminación informática”, núcleo esencial del derecho de Habeas Data, pero aclara que “Aante la posibilidad de acceso a múltiples bases de datos personales (publicadas ahora en la Internet), el fortalecimiento del poder informático (caracterizado por su titularidad en ocasiones anónima), y la carencia casi absoluta de controles, se han incrementado los riesgos de vulneración efectiva no sólo del derecho a la autodeterminación informática, sino de los demás derechos fundamentales puestos en juego en el ámbito informático: la intimidad, la libertad e incluso la integridad personal”.

Este pronunciamiento se hace cuando no existía aún la Ley de habeas Data Sectorial para datos personales financieros de 2008, y cuando se reclamaba por la Corte como lo había hecho en reiterados fallos, que el Congreso debía expedir una ley estatutaria de habeas Data, pues si bien existía el mecanismo de la acción de tutela para garantizar y defender los derechos fundamentales de forma efectiva, no era suficiente pues la regulación de mecanismos de defensa del habeas data debe ser integral de todos los datos personales que se producen en la vida diaria y no solo los financieros, por más de que éstos sean los más relevantes y con valor económico.

La Corte en estas condiciones establece la autonomía de tres derechos fundidos en el artículo 15, constitucional de la siguiente manera: “En la actualidad y a partir de los enunciados normativos del artículo 15 de la Constitución, la Corte Constitucional ha afirmado la existencia-validez de tres derechos fundamentales constitucionales autónomos: el derecho a la intimidad, el derecho al buen nombre y el derecho al *habeas data.* En este último sentido, *“La Corte ha entendido el habeas data como un derecho autónomo, como una garantía y como un derecho-garantía. Si bien en estricto rigor, se trata de la garantía de los derechos a la autodeterminación informática y a la libertad, ante la ausencia de normatividad tanto sustantiva como procesal, y para efectos de su justiciabilidad por parte del juez de tutela, se entenderá como un derecho-garantía en los términos de la sentencia T-307 de 1999”.*

4. LA INTIMIDAD O "LA VIDA PRIVADA" EN EL CODIGO NACIONAL DE POLICIA

Los decretos-leyes 1355 de 1970 y 522 de 1971, configuran el Código de Policía Nacional (CNP), que regula todo lo atinente a las contravenciones generales y especiales, las autoridades competentes para investigar y juzgarlas, así como los procedimientos policivos penales o contravencionales. Ya hemos dicho que la conducta o hecho punible se divide en delitos y contravenciones, y que como tal, al ser una modalidad la contravención de conducta punible se rige por los parámetros generales atribuible a dichas conductas y en lo particular a las directrices, principios, estructuración de las contravenciones, regímenes de culpabilidad y exculpación, y procedimientos policivos contravencionales estipulados en el decreto 522 de 1971, artículos 71 y siguientes.

El CNP, bajo el bien jurídico tutelado de la "Integridad personal", protege la "vida íntima o privada" de las personas y en los artículos 45 a 49, estructura varias contravenciones especiales de competencia de los Alcaldes e Inspectores de Policía, en primera instancia; y de los Gobernadores en segunda Instancia.

Las contravenciones especiales son: (1) Averiguación de la vida íntima o privada, como contravención especial básica (artículo 46-1 CNP); (2) Averiguación de la vida íntima o privada, por medio de grabación, fotografía o "*cualquier otro medio subrepticio*", como contravención especial agravada (artículo 46-2 CNP); (3) Descubrimiento o divulgación de la vida privada o íntima, como contravención agravada de las contravenciones previstas en los numerales 1 y 2 (artículo 47-1 Ibid); (4) Descubrimiento o indiscreción con provecho personal, como contravención agravada de las contravenciones previstas en los numerales 1 y 2 (artículo 47-2 Ibid); (5) Descubrimiento o indiscreción por reincidencia, como contravención agravada de las contravenciones previstas en los numerales 1 y 2 (artículo 47-2 Ibid); (6) Indiscreción de la vida privada "ajena" sin justa causa, como contravención especial básica (artículo 48-1); (7) Indiscreción de la vida privada "ajena" sin justa causa y con provecho personal, como contravención especial agravada (artículo 48-1).

Así mismo, el CNP, bajo el bien jurídico tutelado de la "Propiedad", se protege la "intimidad domiciliaria" en el artículo 56, con las siguientes contravenciones especiales, a saber: (1) Presencia injustificada en habitación ajena o sitios asimilados a ésta que no estén abiertos al público (artículo 56-1 CNP); y (2) Presencia injustificada en habitación ajena o sitios asimilados a ésta, por reincidencia (artículo 56-2 CNP).

Ahora hagamos un breve análisis de cada una de estas contravenciones especiales:

4.1. CONTRAVENCIÓN ESPECIAL BÁSICA: DE AVERIGUACIÓN DE LA VIDA "ÍNTIMA O PRIVADA"

4.1.1. Fuente Normativa: Artículo 46-1 del Código Nacional de Policía o CNP.

"El que sin facultad legal averigüe hechos de la vida íntima o privada de otra persona, incurrirá en multa de cincuenta a cinco mil pesos".

4.1.2. Concepto de "Vida íntima o privada" El concepto de vida privada es plurivalente, atendiendo a diversidad de factores intrínsecos de la persona humana, como de la espiritualidad, las ideas o pensamientos, la moralidad, la ética, el comportamiento individual, familiar o social; o bien en relación del ser humano con otros, atendiendo a los usos y costumbres familiares, vecinales, citadinas o regionales; o bien, el ámbito de interrelación de la persona con la sociedad, atendiendo a factores educativos, ambientales, políticos,

culturales, económicos, antropológicos, etc.; o bien en el ámbito de interrelación de la persona humana como sujeto de derechos y obligaciones con el Estado mismo, atendiendo a las normas jurídicas demasiado prohibitivas o restrictivas; o bien, de sana, recíproca y civilizada convivencia; o bien en el ámbito de interrelación entre Estados, que exista aceptabilidad o no de estatutos normativos internacionales, tratados o convenios bi o multilaterales, que a su vez, recojan o no, incorporen o no, directrices o principios sobre la vida privada de las personas en sus ordenamientos jurídicos internos, no solo dichos predicamentos, con efectos jurídicos sino que los interioricen en su vida diaria personal y familiar y el Estado garantice su respeto y cumplimiento por parte de los asociados como por el Estado mismo.

A partir de la Constitución de 1991, Colombia es un Estado Social de derecho, que entre otros fines, sirve a la comunidad, promueve la prosperidad general y garantiza "la efectividad de los principios, derechos y deberes consagrados en la Constitución", y sus autoridades "están instituidas para proteger a todas las personas residentes…, en su vida, honra, bienes, creencias y demás derechos y libertades, y asegurar el cumplimiento de los deberes sociales del Estado y de los particulares" (artículo 2º constitucional).

El Estado colombiano como sujeto de derecho internacional ha ratificado varios Convenios y tratados públicos (artículo 93 Ibid) y los ha incorporado como fuente de interpretación del derecho y a la legislación interna. En esta segunda opción, con "prioridad en el trámite" [32], cuando se refieran a "proyectos de ley aprobatorias de tratados sobre derechos humanos que sean sometidos a su consideración por el Gobierno" (artículo 164 id).

Preconstitucionalmente a 1991, el Estado Colombiano incorporó a su ordenamiento jurídico vigente y mediante las leyes 74 de 1968 y la 16 de 1972, "El Pacto Internacional de Derechos Civiles y políticos" o Pacto de New York" y *"La Convención Americana Sobre Derechos Humanos o Pacto de San José de Costa Rica,* respectivamente. Las dos normas internacionales son de idéntico tenor a *La Declaración Universal de los Derechos del Hombre*, de 10 de Diciembre de 1948, cuando de la protección de la "vida privada" de las personas se trata. Aunque no se define la vida privada, la conceptualización a la misma se deduce de lo siguiente:

1) El ser humano en su "vida privada" no será objeto de ataques o injerencias arbitrarias, ilegales o abusivas;

2) Existen elementos que estructuran la "vida privada" en el concepto de familia, domicilio, las comunicaciones y la honra y reputación de las personas; y,

3) El Estado a través de leyes está obligado a la protección del derecho a la vida privada de las personas contra toda injerencia o ataque.

Por lo tanto, la vida privada de las personas es un derecho plurivalente, autónomo, subjetivo, reconocido por las normas internacionales e internas de los países y de protección y garantía obligatoria de los Estados y de las personas mismas que los integran.

---

(32) Según el art. 217 de la Ley 5ª de 1992 (Estatuto del Congreso), los aspectos relevante del trámite de estos proyectos son: "Podrán presentarse propuestas de no aprobación, de aplazamiento, de reserva respecto de los tratados y convenios internacionales. El texto de los tratados no puede ser objeto de enmienda. Las propuestas de reserva sólo podrán ser formuladas a los tratados o convenios que prevean esta posibilidad o cuyo contenido así lo admita. Dichas propuestas así como las de aplazamiento, seguirán el régimen establecido para las enmiendas en el proceso legislativo ordinario. Las Comisiones competentes elevarán a las plenarias, de conformidad con las normas generales, propuestas razonadas sobre si debe accederse o no a la autorización solicitada".

Por su parte, los estatutos normativos internacionales europeos y los de los países miembros de la Unión Europea (UE), regulan el derecho de la "vida privada" como sinónimo de derecho a la intimidad, aunque en el derecho español, más aún se distingue aunque solo fuere conceptualmente y en la Exposición de Motivos de la Ley Orgánica reguladora del Tratamiento automatizado de Datos personales o LORTAD de 1992, entre "privacidad" e intimidad, argumentando que la primera, "*constituye un conjunto, más amplio, más global, de facetas de la personalidad que aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado*" **[33]**.

El AConvenio de Europa@, acordado por el conjunto de Estados europeos de la UE, en Enero 28 de 1981, relativo a la *protección de las personas en relación con el tratamiento automatizado de datos de carácter personal,* constituye junto a las Recomendaciones del Consejo de Cooperación y Desarrollo Económico (OCDE, creado en 1948, como organización de cooperación preferente económica entre los Estados Europeos, EE.UU., Canadá, Japón, Finlandia, Australia y Nueva Zelandia) de Septiembre de 1980, por la cual *se formulan directrices en relación con el flujo internacional de datos personales y la protección de la intimidad y las libertades fundamentales;* así como las Directivas 95/46/CE y 97/66/CE, del Parlamento y Consejo Europeo, relativos *al tratamiento y circulación de datos personales, la transmisión electrónica o telemática de datos y la protección al derecho a la intimidad,* conforman, lo que bien podríamos llamar la Constitución Europea relativa a los datos personales procesados por medios, técnicas y procedimientos informatizados, electrónicos o telemáticos. Estas normas emplean indistintamente los términos intimidad y vida privada, a los efectos de protección de las personas, cuando se están tratando por medios informáticos, electrónicos y telemáticos datos que le conciernen a la persona, con lo cual la vida privada en éstos ámbitos incorpora unas nuevas formas de injerencias o ataques devenidas del surgimiento de las tecnologías de la comunicación y de la información o medios TIC, que vinculan a la informática (en computadores interconectados por redes de comunicación internas), electrónica (v.gr. el fax) y telemática (video chat, e-mails, video conferencias, páginas de WEB, páginas HTML, comunicación computarizada: sonido y video, etc.).

En consecuencia y según aquellas normas europeas, aún vigentes, el concepto de vida privada o "intimidad", se replantea así:

1) Es un derecho autónomo previsto en normas europeas (Directivas del Consejo de Europa), como en las Constituciones de los Estados miembros de la UE; también un derecho autónomo, subjetivo porque se considera de aquellos personalísimos, es transnacional, regulado por normas de carácter iuscivilista, administrativista y como *última ratio* por normas penales; y,

2) Es un derecho de la persona humana susceptible de ser vulnerado a través del tratamiento "automatizado" (o mejor, informático, electrónico o telemático) de datos personales. Estos se entienden, como "cualquier información relativa a una persona física identificada o identificable ("persona concernida", como insiste el Convenio Estrasburgo). Se deduce de esta definición, que el concepto de *persona concernida*, a los efectos de determinar de identificación dentro de un procedimiento informatizado de datos, no solamente abarca los rasgos de identificación de la persona de carácter jurídico (como los registros de nacimiento,

---

(33) "…la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona –el domicilio donde realiza su vida cotidiana, las comunicaciones en las que se expresa sus sentimientos, por ejemplo—". AA.VV. ***Colección de discos compactos de Aranzadi***. Ed. Aranzadi, Pamplona, 1997.

médico, etc., documento de identificación personal v.gr., Documento Nacional de Identidad DNI en España o Documento de Identidad Nacional DIN o Cédula de ciudadanía en Colombia, Pasaportes, etc.), sino también de carácter físico interno v.gr., exámenes de sanguíneos, de líquidos humanos diferentes a la sangre (semen, orina, etc.), exámenes morfológicos (color de piel, facial, dentales, ópticos, de estatura, etc.); o de carácter físico externo, con fotografías y huellas humanas y/o tecnológicas (códigos, password o firmas digitalizadas). Estas huellas, se consideran como rasgos diferenciadores de una persona humana de carácter morfológico o tecnológico con incidencia jurídica [34].

En el artículo 15 de la Constitución de 1991, se regula la protección y garantía efectiva del derecho de la Intimidad, como un derecho fundamental, autónomo, de aplicación inmediata por el mecanismo de la acción de tutela y sin necesidad de regulación legislativa sobre la materia. Quizá por esa connotación constitucional que la dio el artículo 83 constitucional, fue por lo que hasta el momento no se ha dictado una ley integral sobre el derecho a la intimidad, que persiga su protección iuscivilista o administrativista, aunque existen normas dispersas que regulan parcialmente el mentado derecho o inmerso en otros derechos correlativos como el Habeas Data (Ley 1266 de 2008, sobre los datos personales financieros); o en forma parcial, en normas de *última ratio* en el Código Penal Colombiano, relativo a los delitos de la violación a la intimidad, reserva e interceptación de comunicaciones (arts. 192 a 197).

Preconstitucionalmente a 1991, el CNP de 1971, determinó que la "vida íntima o privada" como derecho de las personas podría ser vulnerado por diferentes medios tradicionales, "subrepticios" (medios ocultos o a escondidas) y tecnológicos (grabaciones de voz, sonido o imagen) y por diversos intereses de las personas (patrimoniales o extrapatrimoniales), y que por tanto debía ser objeto y fin del Estado su protección elevándolo a contravención especial de competencia de autoridades administrativas de policía, como son los Alcaldes, Inspectores de Policía y Gobernadores, mediante un procedimiento policivo especial que podría terminar con decisión final de privación de la libertad por arresto de los culpables o multas, aunque éstas últimas por no haberse actualizado los artículos 46 a 49 del Decreto-ley 522 de 1971 (integrante del CNP), resultan irrisorias por su desactualización y realidad económica del momento.

En este texto, tampoco se da un concepto de vida privada, pero sí sus elementos de configuración: 1) Existen "hechos" de la "vida íntima o privada" que son objeto de sanción que puede ir desde la multa hasta el arresto del culpable, sí la persona que los "averigua", toma su conocimiento, los divulga por cualquier medio, lo hace por sólo conocerlos o por obtener algún provecho o lucro, sin tener facultad legal para ello;

2) Los hechos de la vida íntima, son aquellas circunstancias de modo, tiempo y lugar en las que ocurren acciones, obras, gestiones, diligencias y sucesos de la vida de una persona que le pertenecen o conciernen y que no van en contra de las demás personas o no constituyen formas delictivas preparatorias o de consumación en contra de los seres humanos o sus bienes. Así mismo constituyen hechos de la vida íntima de la persona, los aspectos intrínsecos (Espiritualidad, religiosidad, creencias, pensamientos, ideas, sexualidad, grados de intelectualidad: "coeficiente intelectual", etc.) o extrínsecos (o físicos: estatura, color de piel, rasgos físicos característicos, "discapacidades" físicas o psíquicas exteriorizadas, estructuración morfológica, sanguínea, etc.).

Los hechos, sucesos, acciones u obras de la vida íntima de las personas obtendrán tutela jurídica efectiva, solo aquellos que están conforme al ordenamiento jurídico vigente, pues aunque

---

(34). RIASCOS GOMEZ, Libardo Orlando. ***El Habeas Data: Visión constitucional, visión legal y en proyectos de ley Estatutaria.*** **En:** http://akane.udenar.edu.co/derechopublico

no lo diga expresamente las normas del CNP al elevar a contravenciones especiales varias conductas humanas en contra de la “vida íntima o privada”, de suyo se excluyen de la protección y garantía contravencional, los hechos ilícitos constitutivos de contravención o delito aún argumentando sus titulares que hacen parte de la vida íntima o privada de aquellas personas, pues sobre ellos, si alguien tiene toma conocimiento por cualquier medio tradicional o tecnológico de su comisión, debe denunciar ante las autoridades, según lo dispone el artículo 27 del Código de Procedimiento Penal, si se trata de conductas delictivas que deban investigarse de oficio, bien presentar querella si la conducta delictiva o contravención así lo exigen. En el caso de las contravenciones especiales incluido este tipo básico de contravención estudiada, exige querella.

3) Existe una dosimetría contravencional que incide en una escala de sanción mínima o grave, en atención al proceso de averiguación, conocimiento y divulgación de los hechos de la vida íntima o privada de las personas. En efecto, si sólo se averigua hechos de la vida privada, sin “facultad legal” para hacerlo, obtendrá una sanción de multa; pero si se recurre a medios tecnológicos o subrepticios, la sanción de multa aumentará hasta en la mitad más, y así sucesivamente hacia arriba hasta llegar a una sanción de arresto en la última etapa del procedimiento de conocimiento de los hechos de la vida privada que es la divulgación o indiscreción con provecho o lucro. Esto supone entonces que, no existe contravención si se “averigua”, conoce o divulga hechos de la vida privada, sí el agente actúa con “facultad legal”, es decir, con autorización legal o judicial. V.gr. autoridades judiciales con ocasión de sus funciones de investigación o juzgamiento, personas que realizan funciones de policía judicial con autorización judicial, profesionales médicos, abogados, investigadores privados, profesionales de la salud (médicos clínicos o quirúrgicos, enfermeros, farmaceutas, fisioterapeutas, odontólogos, etc.).

4) Los hechos que hacen parte de la vida íntima o privada de las personas, por no hacer distinción las normas del CNP., se entenderán desde los simplemente anodinos hasta los que tienen valor o relevancia jurídica, económica o de otra índole. El límite a los hechos de la vida privada como derecho constitucional no absoluto, serán los hechos de la vida pública, el derecho de los demás, el no abuso de los propios y el ordenamiento jurídico vigente.

También se puede decirse, que constituye un autolímite de los hechos de la vida privada, los hechos que aún siendo privados tienen un verdadero interés general o público, de transparencia antes que de secreto o sigilo generalizado (excepto, los que establece el ordenamiento jurídico vigente, tales como la Seguridad, Integridad, defensa, Industria, Salubridad del Estado), como sucede con los servidores del Estado que en el momento de tomar juramento de su cargo juran cumplir y respetar la Constitución, las leyes y demás normas jurídicas y cumplir fielmente sus funciones, deberes y no extralimitar o abusar de ellos (artículos 2, 6, 122 a 130, constitucionales) y eso implica que su vida privada puede verse restringida por el desempeño de sus funciones y su status funcionarial los cuales afectarán entre otros hechos, sucesos, acciones, obras o condiciones personales y familiares, tales como: (i) su seguridad personal y familiar; (ii) sus traslados, horarios y lugares de desplazamiento; (iii) sitios para vacacionar él y su núcleo familiar; (iv) escogencia de los establecimientos de estudio del núcleo familiar; (v) derechos de visita a familiares, vecinos y amigos; (vii) establecimientos de atención médica, farmacéutica, quirúrgica, estética, dietética, deportiva, etc..; (iv) actividades que no siendo ilícitas y no afectando a la condición de servidor del Estado, sólo son de conocimiento del funcionario estatal y su personal de seguridad.

También se convierten en autolímite de la vida privada aquellos hechos que siendo privados en su origen, deben ceder al interés general o público pues es allí donde cobran verdadero interés y efectos principalmente positivos, aunque no se destaca los de carácter negativo o violatorios de la vida privada o íntima de las personas, si se hace sin el consentimiento del

titular expresa o tácita (con señas o asentimientos corporales). En efecto, sucede con grandes personajes de la literatura, la política, la farándula, el teatro, el cine, actividades mercantiles entre otras, en donde el interés de la colectividad prima sobre la vida privada, cuando publican bibliografías, obras de literatura, de teatro, de cine, Pinturas, fotografías (análogas y digitales) o extractos de la vida privada en periódicos, diarios, revistas o medios informáticos, electrónicos o telemáticos; y en fin, hechos de la vida privada debidamente autorizados.

También podríamos encontrar el límite jurídico a los hechos de la vida privada, en el derecho a la información que tiene toda persona, a ser informado en forma veraz, oportuna e imparcial (artículo 20, constitucional).

4.1.3. Sujeto activo de la contravención. Puede serlo cualquier persona sin connotación alguna, lo cual significa que podrá ser también un servidor público, sin embargo, las normas del CNP., nada refieren a esta cualificación del sujeto activo que por obvias razones debería provocar una dosimetría contravencional sancionatoria mayor que si la conducta es cometida por una persona particular. Esto por cuanto, según el artículo 6 y 122 constitucionales, los servidores del Estado responden no sólo por la vulneración del ordenamiento jurídico vigente, sino por la acción, omisión y extralimitación de funciones públicas.

Aunque el artículo 104 del Decreto-ley 522 de 1971, sostiene que en caso de no hallar norma precisa sobre la materia, por remisión legal deberá aplicarse el Código de Procedimiento Penal. En este caso, se debería aplicar las causales de agravación punitiva por la condición del agente o sujeto activo de la contravención (Servidor estatal), del artículo 58 del Código Penal Colombiano (Ley 599 de 2000), pues su excepcional condición provoca una privilegiada actuación digna de mayor punibilidad contravencional, a menos que el servidor del Estado actúa con "facultad legal", con lo cual de suyo destipificaria la conducta.

4.1.4. Verbo rector del tipo contravencional. "Averiguar", según el diccionario, significa inquirir o indagar la verdad hasta descubrirla. Esto significa que la averiguación de los hechos de la vida privada de la persona concernida deben ser lo que se ajustan a la verdad, pues de lo contrario, podríamos estar cayendo en otra figura contravencional o en un delito de injuria o calumnia (artículos 220 y ss. Del Código Penal), si no sólo averigua los hechos no verídicos de la persona concernida, sino que hace imputaciones deshonrosas o impute falsamente a otro una "conducta típica" (delito o contravención).

4.2. Contravención especial agravada de averiguación de la vida íntima o privada cuando se realiza con medios tecnológicos o "subrepticios"

4.2.1. Fuente Normativa. Artículo 46-2 CNP. "*Si la conducta* (la verificada en el artículo 46-1Ibid) *se realiza por medio de grabación, fotografía o cualquier otro mecanismo subrepticio, la multa aumentará hasta en la mitad"*.

4.2.2. Razones insuficientes para la agravación contravencional. La norma policiva en el inciso 2º , realmente establece una forma de agravación del tipo contravencional basada en un aspecto equívoco, pues si la averiguación de la vida íntima o privada de una persona, sin "facultad legal" se verifica utilizando cualquier medio de pesquisa de información o hechos de la vida privada, los cuales pueden ir desde las simples escuchas, tras las puertas, ventanas o paredes, pasando por las grabaciones de voz, sonido o imagen con aparatos eléctricos o electrónicos tradicionales (cámaras de video, de fotografías, radio-teléfonos, etc.) hasta los más sofisticados y tecnológicos que incluyan los modernos medios TIC, de informática, electrónica o telemática (equipos computaciones unidos a través de redes de redes de información como la Internet, en los que interactúan informaciones o datos de voz, imagen y sonido: v.gr. conferencias telefónicas por internet, con sonido e imagen en tiempo real, con

software idóneo para aquello: v.gr. skipe). Dentro de estos medios modernos de comunicación e interceptación a la misma, por ejemplo, el "*Wardriving*" que es una búsqueda de información a través de redes inalámbricas Wi-Fi desde un vehículo en movimiento. Implica usar un "carro" y un ordenador equipado con un computador portátil o un PDA (o computador de mano), para detectar las redes. Esta actividad es parecida al uso de un escáner para radio. Y unos y otros están previstos en los términos utilizados en dicho inciso, bajo los términos ***"mecanismos subrepticios"***, pues estos se entienden los "artefactos, aparatos o dispositivos informáticos, electrónicos, telemáticos o manuales con los que "se hace o toma ocultamente y a escondidas" una imagen, un dato, voz o información personal.

4.2.3. Medios de Policía. Las autoridades de policía nacional, departamental, distrital y municipal para ejercer su poder policivo de conservación, protección y garantía del *orden público* (que abarca, la tranquilidad, seguridad, moralidad públicas y el ornato y medio ambiente) y las libertades constitucionales y legales de carácter público – como la locomoción, la residencia, la reunión, el comercio e industria, la propiedad y los espectáculos- debe utilizar unos medios policivos que permiten cumplir dichas funciones garantistas en la sociedad, por ello, como lo afirma *Oliver Bonilla* [35], los medios de policía deben observar los siguientes principios: (i) …están subordinados a la Constitución y las leyes; (ii)…no pueden ser incompatibles con los principios humanitarios; (iii) En la conservación del orden público el fin no justifica los medios; (iv) La omisión o extralimitación en el empleo de los medios de policía, hace responsable al agente.

Los medios de policía previstos en el CNP (Decreto-ley 1355 de 1970), artículos 7 y ss., son los siguientes: (i) Los reglamentos, (ii) los permisos, (iii) las órdenes, (iv) del empleo de la fuerza y otros medios coercitivos, (v) del servicio de policía, (vi) de la vigilancia privada, (vii) la captura, (viii) del domicilio y su allanamiento, y (ix) la asistencia familiar. Ahora bien, resulta aplicable a la contravención especial del tipo básico como el agravado, lo preceptuado en el artículo 55 del CNP, sobre los medios de policía de "vigilancia privada", pues se sostiene: "la *vida íntima de personas ajenas a sindicación penal (o mejor investigación por autoridades competentes) no podrá ser objeto de investigación privada o judicial. Sin embargo, podrán realizarse indagaciones privadas con fines laborales o comerciales*". Lo cual supone que está prohibida cualquier investigación de la vida íntima o privada de las personas en su diario vivir, salvo que estén vinculadas a una investigación de índole penal o contravencional, o se realicen con "fines laborales o comerciales".

Pese a que el artículo 55 mentado, posibilita dichas prácticas, creemos que son violatorias del derecho a la intimidad y la buena imagen en el sitio de trabajo, o en cualquier lugar, con fines publicitarios (artículo 15, constitucional). Ni el Código Laboral ni el de comercio han reglamentado dichas prácticas como usuales para mejorar las actividades en los sitios de trabajo ni tampoco como potenciar la imagen de las personas que presten sus servicios para fines publicitarios. Como dijéramos en otra obra nuestra [35A], en la última década [36],el empleo

---

(35) OLIVER BONILLA, Leonel. ***Derecho de Policía***. Tipografía Central, 2ª edición, Bogotá, 1984, p. 41

(35A) RIASCOS G. Libardo O. ***El Derecho a la Intimidad, visión ius-informática y los delitos relativos a los datos personales***. Tesis Doctoral, Universidad de Lleida, Lleida (Esp.), 1999, p. 560 y ss.

(36) La "*Video Surveillance*", como industria en la Gran Bretaña, ha recibido entre 150 y 300 millones de libras, al instalar unas 300.000 cámaras para los sistemas de CCT, en diferentes sitios públicos y privados. Los diferentes impactos que ha ocasionado el adelanto técnico y sus constantes colisiones con los derechos fundamentales, se ha visto reflejado en los innumerables casos y escritos sobre el tema. v.gr. a) Testimonio del Director General Simon Davies ante la Cámara de los Lores, sobre la "Visual evidence and surveillance", Oct. 23 de 1997. b) Perjuicios ocasionados por los dispositivos "CCTV Targets, KDIS On line", Oct. 24/97; c) La "Privacy Internacional" ha aplicado cuestionarios para evaluar los impactos de las CCTV (FAQ: Frequently Asked Questions); d) Reales amenazas mundiales con los sistemas de vigilancia CCTV. Los sistemas de video y transmisión de imágenes con cámaras ocultas y otros dispositivos. En: www.umontreal.edu.ca

De los circuitos o sistemas cerrados de televisión (CCTV. "*Closed Circuit Television*"), inicialmente diseñados para la vigilancia y prevención del delito en centros de educación, bancarios, de salud, instituciones de toda clase, sitios de parqueo y edificaciones públicas y privadas, etc, ha crecido inusitadamente en el mundo y, especialmente, en las grandes ciudades de la Gran Bretaña, Norteamérica, Australia y varios países de Europa.

En efecto, estos mecanismos de almacenamiento, procesamiento y transmisión de información o de datos con imágenes digitalizadas fijas o en movimiento o de vídeo, fueron creados con fines de seguridad y prevención de la sociedad contra posibles actos delictivos. Esta forma de vigilancia se ha convertido en una especie de control social efectivo que refuerza el control policivo. Sin embargo, en la Gran Bretaña estas nuevas tecnologías han causado un gran impacto en la comunidad, más que ninguna otra, principalmente porque se ha visto involucrado la Intimidad ("privacy") de las personas con profundos efectos para las generaciones futuras, tal como lo ha expresado la Oficina de la "*Privacy Internacional*" **[37]**. Impactos que ya se están observando, pues los sistemas de CCTV unidos a la informática (principalmente en el almacenamiento y tratamiento de información digitalizada y/o video), hoy han potenciado su actividad y riesgo frente a los derechos y libertades de la persona.

Concordantemente con lo anterior y en contravía, al menos conceptual con lo previsto en el artículo 55 de CNP, los artículos 72 a 85 ibídem, al reglamentar otro de los medios de policía como es el "allanamiento" y expresa: "*la policía amparará en todo momento la inviolabilidad del domicilio y de sitio no abierto al público, con el fin de garantizar a sus moradores, la protección a la intimidad a que tienen derecho*", y agrega: "*El acceso al domicilio o a sitio privado donde se ejerza trabajo o recreación familiar, requiere consentimiento de su dueño o de quien lo ocupe*".

Si se considera, entre otros, y para fines del CNP, "domicilio,…las oficinas, talleres y los demás recintos donde trabaja…"y éstas están amparadas por el ordenamiento jurídico vigente a no violentarse por ningún medio tradicional o tecnológico, mal se puede afirmar que quedan habilitadas las indagaciones de la vida privada con fines laborales o comerciales. Estas prácticas indagatorias, como se ha dicho desconocen los artículos 2 y 15, constitucionales porque vulneran el núcleo duro de la "privacy", la vida privada y su desenvolvimiento en la vida de hogar, personal y familiar de las personas, donde se lleva a cabo, lo más íntimo de las personas, la ideación y realización de sus sentimientos y pensamientos, creencias, religiosidad o espiritualidad, etc., y si esos datos personales son recogidos, almacenados, registrados y transmitidos (o divulgados), sin el consentimiento de los concernidos, constituirán tipos delictivos y constituirán "circunstancias de mayor punibilidad" (art. 58-3 C. Penal), como veremos más adelante.

El Convenio de Estrasburgo de 1981, seguido muy de cerca por la LORTAD de 1992 y 1995 en España, establece prohibiciones a la recolección y tratamiento informatizado de datos personales de "datos sensibles" o integrantes del núcleo duro de la intimidad, tales como los relativos a la vida sexual, el origen racial, la salud, las creencias, la ideología, entre otros, y sólo por excepción se permitirá dicho tratamiento o procedimiento informático, previa disociación de los datos que permitan no identificar a las personas concernidas y se haya obtenido su consentimiento sólo con fines estadísticos.

---

(37) "Video Surveille". La sede principal de la Oficina por el derecho a la Intimidad está en la Gran Bretaña. Esta Oficina se ha constituido como una institución con ámbito global, con especial énfasis en los países de la Common Wealth, para la defensa de la Intimidad, sea cual fuere los mecanismos, instrumentos o equipos o aparatos de la tecnología TIC en unión con la informática, que se utilicen como posibles medios (mecánicos, eléctricos, electromagnéticos visuales o audio-visuales) para la comisión de un delito o infracción de carácter administrativo. En: www.umontreal.edu.ca

4.3. Contravención especial de descubrimiento o divulgación de la vida privada o íntima, como contravención agravada de las contravenciones previstas en los numerales 1º y 2º del artículo 46 del CNP.

4.3.1. Fuente Normativa. Artículo 47-1 CNP. "El que divulgue los hechos a que se refiere el artículo anterior, incurrirá en multa de cincuenta a cinco mil pesos".

4.3.2. El bien jurídico tutelado y el sujeto activo. Al igual que la contravención especial básica y agravada prevista en el artículo 46 del CNP., la presente se halla bajo el bien jurídico tutelado de la "Integridad personal" en la vertiente no física, pues en la física el CNP, coloca la contravención de omisión o ayuda a personas heridas o en peligro de muerte o de grave daño a su integridad personal (artículo 45 ibíd.). Sin embargo, como *ut supra* se ha dicho, las contravenciones contra la vida privada o íntima, pudieran estar mejor ubicadas bajo el bien jurídico autónomo de la Intimidad o de la "libertad y otras garantías" como lo estipula el Código Penal de 1980 y 2000, aunque en éste último es cuestionable, como lo comenta *Morales Prats* [38], en el ámbito del derecho español, pues desconoce la autonomía de la intimidad, no solo como derecho constitucional, autónomo sino como bien jurídico con valor e interés general que lo hace digno de reconocimiento y protección jurídico penal, pues no es suficiente incluir a los delitos contra la intimidad, los secretos o confidencialidad y la inviolabilidad de domicilio, bajo un bien jurídico genérico de la Libertad, pues así se pierde coherencia y verdadera sistematización de un derecho-bien jurídico que tiene identidad propia y merece garantía efectiva de la ley penal.

Esto mismo, podemos argumentar para el actual Código Penal de 2000, que siguió protegiendo a la intimidad bajo un título genérico de la libertad y otras garantías, junto a otros delitos que no guarda coherencia o agrupación sistémica con la intimidad y la confidencialidad de algunos secretos personales, pues la inviolabilidad de domicilio se halla en bajo otro bien jurídico, como veremos *ut infra.*

El sujeto activo en esta clase de contravenciones agravadas contra la vida privada de las personas puede ser cualquier persona. Al igual que en las contravenciones anteriores, no se prevé la mayor punibilidad, porque la cometan servidores públicos, fuera de las facultades o atribuciones que les competen, lo cual encontraría respaldo en la Constitución (artículos 2, 6 y 122), como en el C. Penal., artículo 58-8.

4.3.3. Verbo Rector. "Divulgar". Divulgar es "publicar, extender, poner al alcance del público algo". La divulgación de hechos, datos o informaciones de la vida privada, se puede realizar a través de medios orales, radiales, vía telefónica, vía fax, por medios de medios de prensa escrita (periódicos), revistas generales, especiales, científicas, etc., magazines (Publicación periódica con artículos de diversos autores, dirigida al público en general), o bien medios de comunicación y de información TIC, que utilicen medios comisivos informáticos, electrónicos o telemáticos (voz, audio e imagen presentados por equipos computaciones e interconectados en red, a través de la Internet).

Estos últimos resultan medios comisivos más invasivos, porosos y penetrantes de la vida privada, no sólo por la inmediatez (a la velocidad con la que viaja la información en la Internet) de la divulgación o indiscreción de los hechos, datos o informaciones de la vida privada, sino por la circulación o transmisión de datos personales en un ámbito transfronterizo o global y no simplemente en el contorno de la "aldea" donde se producen los hechos, datos o informacio-

---

(38) AA.VV. ***Comentarios a la parte especial del Derecho Penal.*** Editorial Aranzadi, Pamplona, p. 294 y ss.

nes, como pudiera suceder antes de la irrupción de la informática en la vida actual, con los medios tradicionales de comunicación e información, como la conversación oral, la radio, la prensa y las revistas, entre otros.

4.4. Contravención especial de descubrimiento o indiscreción con provecho personal, como contravención agravada de las contravenciones previstas en los numerales 1 y 2 del Artículo 46-1 Ibid

4.4.1. Fuente normativa. Artículo 47-2 Ibid "Si de tal divulgación se obtiene provecho personal, la multa se aumentará hasta en la mitad"

4.4.2. Bien jurídico tutelado, sujeto activo y conceptualización del verbo rector. Todo lo manifestado en la contravención especial agravada anterior y sobre estos temas es válido para la presente modalidad de contravención.

4.4.3. "El provecho personal", como causal de agravación de la contravención especial.

El provecho, es el "*beneficio o utilidad que se consigue o se origina de algo o por algún medio*". Con lo cual, el "provecho" es un término equivoco que puede abarcar a diferentes clases de beneficios o utilidades que van desde los casi intrascendentes hasta los más complejas que involucren aspectos patrimoniales, crematísticos o rentísticos. Ahora bien, el término "personal", aunque parecería un límite al término "provecho", consideramos que no es así, porque si el beneficio como tal puede ser multicomprensivo (inmaterial o material), el término personal, solo hace alusión a la persona que obtiene ese beneficio para sí para un tercero. De allí que se entienda que el provecho personal puede ser de carácter inmaterial (por obtener oscuros e íntimos datos, hechos o informes de una persona para satisfacción personal o de terceros que eventualmente los explote en satisfacción de tipo sexual, profesional o de poderío informativo ("Hackers") que él solo pudo tomar conocimiento y divulgarlo por la red de redes o internet, por ejemplo); o de carácter material, que generalmente es económico, patrimonial o crematístico.

Frente a esta anfibología del término provecho, hubiese sido más conveniente que se estableciera en forma inequívoca que la causal de agravación de la contravención deba realizarse con "fines lucrativos", para entender que sólo pueda darse la contravención agravada por fines netamente crematísticos.

Es criticable también la causal de agravación por "fines lucrativos", porque lo que se persigue en esta clase de contravenciones es proteger un derecho subjetivo o personalísimo como la "vida privada" y esta no puede deformarse adicionándole un elemento patrimonial, además de la dificultad de la prueba ya en el transcurso de la investigación que implica poder probar si hubo o no provecho económico.

4.5. Contravención especial de descubrimiento o indiscreción de los hechos de la vida privada por reincidencia.

4.5.1. Fuente Normativa. Artículo 47-3 Ibíd. "*En caso de reincidencia, la pena será de uno a seis meses"*.

En la presente contravención es válido el tratamiento doctrinal y temático que le hemos dado a las dos anteriores contravenciones especiales.

4.5.2. La reincidencia como "causal de agravación punitiva". Fue generalizado escuchar que el tema de la "reincidencia" había desaparecido del Código Penal y por tanto al seguirse previendo la reincidencia en el CNP, esta resultaba contraria al ordenamiento jurídico vigente.

En tal virtud, se demandó el artículo 63 del CNP, que sostiene: ***"****El que después de una sentencia condenatoria cometiere una nueva contravención, incurrirá en la sanción que a esta corresponde* ***aumentada en una cuarta parte para la primera reincidencia y en una tercera parte para los demás****, siempre que la nueva contravención se haya cometido antes de transcurrido dos años de ejecutoriada la condena. La regla anterior dejará de aplicarse cuando en disposición especial se prescriba tratamiento diferente*".

La razón principal de la demanda era por violar el artículo 29, constitucional al desconocer el principio del *Ne bis in idem o non bis in idem, "ya que impone el incremento punitivo por reincidencia como un agravante. Es decir, se establece una doble sanción, es como si se condenase por una conducta distinta un hecho anteriormente cometido, lo cual desconoce que se trata de dos contravenciones diferentes y que por la primera ya se ha cumplido la medida sancionatoria impuesta"*.

La Corte en la Sentencia C-062 de 2005, al refutar estos argumentos estimó: (i) La reincidencia no ha sido derogada del CNP., puesto que está es aplicable a las contravenciones; (ii) La "disposición establece un agravante punitivo que encuentra fundamento no en la comisión de una conducta contravencional, sino en la apatía al cumplimiento de las normas, que se revela a través de la reincidencia y así desestimula la comisión de conductas socialmente reprochables; (iii) el legislador está facultado para expedir los ordenamientos legales que rijan el sistema penal y establecer procedimientos distintos para el juzgamiento de contravenciones y de delitos; (iv) La tarea del legislador al adoptar tales procedimientos, se ve limitada a criterios de razonabilidad y proporcionalidad, pues debe siempre respetar las garantías del debido proceso y del derecho de defensa; (v) La Constitución no tiene mandato concreto que prohíba la reincidencia, ni tampoco en sentido contrario. El legislador penal de 1980, la eliminó al considerar que era "un concepto peligrosista de la sanción" y el legislador del 2000 la revivió para el delito de contrabando".

En consecuencia, siendo la reincidencia un causal de agravación punitiva que tiene como finalidad la persuasión y prevención del infractor contravencional para que no lo vuelva a hacer y que por tanto no ha desaparecido del CNP, es concluyente que esta clase de contravención especial agravada puede válidamente ser sancionada con la pena de arresto de uno a seis meses, tal como lo estipula la parte in fine del artículo 47.

4.6. Apoderamiento y posterior Indiscreción de la vida privada "ajena" sin justa causa, como contravención especial básica.

4.6.1. Fuente Normativa. Artículo 48-1 CNP**.** "El que habiendo tenido conocimiento de un hecho de la vida privada ajena, la divulgue sin justa causa, incurrirá en multa de cincuenta a dos mil pesos".

4.6.2. Falta de técnica legislativa. Esta contravención especial agravada, constituye una reiteración innecesaria de los tipos contravencionales previstos en los artículos 46 y 47 del CNP., que fácilmente pudieran haberse subsanado dándole una mejor redacción al artículo 46 en su primer inciso y los tres incisos del artículo 47.

Quizá en lo único que se diferencia la presente contravención especial de los tipos básicos y agravados de los artículos 46 y 47, es el primer verbo rector con el que inicia su redacción el artículo 48-1, es decir, en el *"tener (por tomar) conocimiento de un hecho de la vida privada*"

que estructura la contravención de “apoderamiento” de los hechos, datos o informaciones de la vida privada de otra persona (que no “ajena” como aparece en la norma) y sin que sea una contravención agravada, dichos hechos apoderados, los deberá divulgar, “sin justa causa” para que se estructure el tipo contravencional pleno, pues los verbos tener y divulgar según la redacción de la norma son consecutivos con términos cualificados adicionales.

En efecto, no basta con apoderarse o “tomar conocimiento” de los hechos de la vida privada, sino que se necesita que los divulgue “sin justa causa” para que se estructure la contravención, pues si sólo se apodera de esos hechos y no procede a ponerlos en conocimiento público por los diferentes medios tradicionales o tecnológicos, de los que antes hemos comentado, el tipo contravencional quedará mutilado y sin estructuración plena. Cosa diferente es que el agente de la contravención proceda a divulgarlos presuponiendo que los tiene en su poder o que ha tomado conocimiento de ellos y esta circunstancia, si los divulga, “sin justa causa”, se habrá encasillado en la norma comentada.

Sin embargo, en este último caso, pudiera alegarse y eso sería válido, que el agente que divulga los hechos de la vida privada de otra persona, no es la que a su vez se apoderó de aquellos y entonces tendríamos dos agentes distintos, el uno que se apodera de los hechos y otro que los divulga.

De otra parte, la falta de técnica legislativa, también se extiende a la utilización de los términos “sin justa causa” que tanto se ha criticado por la Corte Suprema de Justicia al analizar este elemento del injusto penal, *mutatis mutandi* al injusto contravencional. En efecto, la Corte has sostenido que la expresión “sin justa causa, es considerada por un sector de la doctrina como un elemento superfluo, producto de una falta de técnica legislativa, que en nada modifica la descripción de la conducta, pues se refiere a la misma exigencia de la antijuridicidad (que está prevista en la parte general del Código Penal para considera a toda conducta como punible), en tanto que para otros autores, es un elemento normativo del tipo que permite al juez eximir de responsabilidad en causales legales o extralegales, distintas a las de justificación previstas en el artículo 29 del Código Penal” (CSJ., Sentencia Diciembre 4 de 2008).

4.7. Contravención de Apoderamiento e Indiscreción de la vida privada “ajena” sin justa causa y con “provecho personal”, como contravención especial agravada

4.7.1. Fuente Normativa. Artículo 48-2. “Si divulga el hecho con obtención de provecho personal, la multa aumentará hasta en la mitad”.

Sobre la anterior contravención agravada por el “provecho personal”, ya hemos anotado en las anteriores contravenciones. Solo resta decir que el *in extremis* de falta de técnica legislativa en este inciso 2º , se hace evidente al máximo cuando la contravención básica prevista en el inciso 1º ya preveía la divulgación como elemento constitutivo de la contravención y sobraba volver a incluirlo en este segundo inciso, pues la connotación que se haría para que la contravención se considere agravada sería nada más que el “provecho personal”, para que la sanción sea de multa aumentada en la mitad de la prevista en el inciso 1º .

4.8. Contravención de presencia injustificada en habitación ajena o similares

4.8.1. Fuente normativa. Artículo 56-1 CNP

“*El que sea sorprendido dentro de habitación ajena, depósito, granero, caballeriza o cualquier otro lugar destinado a la guarda o custodia de animales u otros bienes, o dentro de tienda o almacén que no estén abiertos al público, y no justifique su presencia en tales lugares,*

incurrirá en arresto de seis a doce meses, si el hecho no constituye delito de violación de domicilio"

4.8.2. Bien jurídico tutelado. Según el Capítulo IX, del Título IV del Decreto- 522 de 1971 o CNP, es el "Patrimonio", pues el legislador de 1971, piensa que lo que debe protegerse por las normas punitivas contravencionales es la propiedad y no la persona que la habita y por ello, la presencia injustificada en habitación ajena o asimilada a éste, se estructura como una contravención especial contra el Patrimonio.

El Código penal del 2000, al igual que lo hizo el C. Penal de 1980, radicó el delito de violación de habitación ajena bajo el bien jurídico tutelado genérico de la "Libertad y otras garantías", en forma autónoma para los delitos de inviolabilidad de habitación ajena o sitio de trabajo, pudiendo aprovechar el cambio de legislación de 2000, para incluir los mentados delitos bajo el bien jurídico tutelado específico de la Intimidad, tal como lo hiciera el Código Penal de 1995, quien en aquella época anunciaba haber superado esa discusión doctrinal de si la violación de morada o "habitación ajena" extendida al "domicilio de las personas jurídicas y establecimientos abiertos al público" (arts. 202 a 204", afectaban a la propiedad o a la libertad genérica de las personas, para ubicarlo en el bien jurídico tutelado de la intimidad, "la intimidad domiciliaria", porque lo que se protegía era esa esfera de la personalidad de carácter subjetivo y no la propiedad (o "Patrimonio") como derecho objetivo, pues éste ya tenía otro apartado en el Código Penal que le dedicaba a plenitud su tutela y protección como tal.

En efecto, sostiene *Morales Prats* [39], "Lo anterior comporta el abandono de propuestas orientadas a la fijación del bien jurídico en la idea de *seguridad personal,* según una tradición jurídica que proviene de la edad media. En el pasado, no han faltado tampoco *formulaciones patrimonialistas* de la inviolabilidad del domicilio, orientadas a considerar que el *ius puniendi* que deriva de la misma es expresión de la propiedad o de la posesión de la morada, tesis que encuentra sus antecedentes en la institución romana *domus disrupta;* estas construcciones teóricas no parecen postulables hoy en día a la vista del tenor del artículo 18.2 CE y de la nueva sistemática por la que ha adoptado el nuevo Código Penal de 1995".

4.8.3. Domicilio según el CNP

Según el artículo 74 del CNP, entiende por domicilio "*los establecimientos de educación, los clubes sociales y los círculos deportivos, los lugares de reunión de las corporaciones privadas, las oficinas, los talleres y los demás recintos donde trabaja; aquella parte de las tiendas y sitios abiertos al público que se reservan para la habitación u oficina; los aposentos de los hoteles cuando hubieren sido contratados en arriendo u hospedaje y las casas y edificios de departamentos estén o no divididos por pasajes*"; por el contrario, no se reputarán domicilio, según el artículo 75 Ibíd., "los lugares públicos o abiertos al público ni los sitios comunales como pasajes, pasadizos y vestíbulos".

Se aclara también, que son "sitios abiertos al público, entre otros, las tabernas, los restaurantes, las salas de bailes y los destinados a espectáculos, aunque para entrar a ellos deban cumplirse condiciones que señale el empresario. Con todo, cuando en sitio abierto al público se establezca recinto de trabajo o de habitación, éste se reputa lugar privado. Terminado el espectáculo o finalizada la tarea en sitio abierto al público, el lugar se torna en privado".

4.8.4. Verbos rectores del tipo contravencional. "Sorprender" o coger desprevenido dentro de habitación ajena o asimilables. La falta de técnica en la redacción de esta contravención especial se vuelve a imponer en este tipo básico, no solo a los efectos del contenido mismo del tipo, sino del uso ambiguo de los verbos rectores "ser sorprendido" o del adverbio

"sorprenderse" que pudieran explicar verbo correcto de "entrar" a una habitación ajena o asimilada a ésta. Quizá esa imprecisión terminológica se deba a poder diferenciarse de la descripción y narración del delito de inviolabilidad de habitación ajena que trae el Código Penal Colombiano, y por eso a riesgo de caer en una especie de bis in ídem normativo como contravención y como delito, una misma conducta, aclara in fine del artículo 56 del CNP, "*si el hecho no constituye delito de violación de domicilio*".

El artículo 189 del C.P. del 2000, estima que se configura delito de inviolabilidad de habitación ajena, así: "*El que se introduzca arbitraria, engañosa o clandestinamente en habitación ajena o en sus dependencias inmediatas…*", destacando de la utilización del verbo rector que lo determinante para que se estructure el tipo penal sólo es entrar arbitraria, engañosa o clandestinamente y no permanecer injustificadamente en dicha habitación.

Por esta razón para diferenciar los tipos penales y contravencionales con relación al domicilio o habitación ajena, preferimos titular la contravención como "presencia injustificada en domicilio" pues lo que importa en esta contravención especial violatoria de la "intimidad domiciliaria" es ser sorprendido dentro de la habitación ajena o asimilables a ésta y éste no "justifique su presencia en tales lugares".

4.8.5. Penas más severas para la contravención de presencia injustificada en domicilio, que las previstas en el delito de violación de habitación ajena prevista en los artículos 189 a 191 del Código Penal de 2000.

Curiosamente siendo teóricamente menos grave incurrir en la contravención especial de presencia injustificada en domicilio ajeno, que en el delito de inviolabilidad de habitación ajena, las penas son más severas par la contravención, porque si se da el supuesto de ser sorprendido en habitación ajena y no justifica su presencia en tales lugares, la sanción será de "*arresto de seis a doce meses*"; en cambio, si se comprueba la comisión del delito de inviolabilidad de habitación ajena, la pena será de "multa".

Más aún la contravención de presencia injustificada de domicilio agravada porque el "agente hubiere sido condenado dentro de los cinco años anteriores por delito contra la propiedad", la sanción se "*aumentará hasta en otro tanto*".

Frente a esta diferente dosimetría sancionatoria, lo previsto en el Código Penal resulta irrisorio. Si bien aquí debe aplicarse los conceptos vertidos por la CSJ de Diciembre 4 de 2008, sobre el elemento del injusto penal "sin justa causa" y sobre la reincidencia (C-062-2005) en las cuales se ratifica la cláusula general de competencia legislativa del Congreso de la República para reglamentar figuras u tipos penales o contravencionales con diferenciación de las instituciones que les son aplicables, no creemos que este principio legislativo se extienda a tipificar tipos contravencionales de parecido contenido a los tipos penales de mayor entidad jurídica con sanciones menores a los tipos contravencionales de menor entidad jurídica. ¿Es jurídica esta anfibología sancionatoria?

4.8.6. Tipo contravencional agravado de presencia injustificada en habitación ajena

El Inciso 2º del artículo 56 del CNP, estipula que la "sanción se aumentará hasta en otro tanto, si el agente hubiere sido condenado dentro de los cinco años anteriores por delito contra la propiedad".

---

(39) AA.VV. ***Comentarios a la parte especial del Derecho Penal.*** Editorial Aranzadi, Pamplona, p. 343 y ss.

Sea lo primero recordar que esta falta de técnica legislativa, es propia del CNP, máxime que desde su expedición en 1971, sobre el particular no se revisado por parte del Congreso de la República como autoridad competente para ello, pero es que tampoco la doctrina ius penalista ha propuesto alternativas para su reestructuración, o el planteamiento de la derogación tácita o expresa de los artículos 46 a 48 del CNP, por la nueva redacción del artículo 189 del C. Penal del 2000, que abarca todos los supuestos de hecho y de derecho de las contravenciones especiales básicas y agravadas antes estudiadas, pero que paradójicamente resultan desde el punto de vista de la sanción irrisorias frente a las previstas en las contravenciones especiales; o si por el contrario, no existe tal derogación expresa o tácita, pues con base en los mismos planteamientos vertidos por la Corte Suprema de Justicia de Diciembre 4 de 2008, el legislador goza del poder legislativo para reglamentar libre e independiente lo atinente a contravenciones o delitos desde la configuración de tipos penales y contravencionales, así como las instituciones jurídicas aplicables a éstas en forma autónoma o por remisión de las propias de los delitos aplicables a las contravenciones; las relativas a sanciones y su dosimetría sancionatoria e inclusive a los procedimientos por los cuales se los investiga y juzga.

5. LA INTIMIDAD DE LAS COMUNICACIONES EN EL CODIGO PENAL DE 1980

En el derogado Código Penal de 1980, dentro del Título X, relativo a los "*Delitos contra la Libertad individual y otras garantías*" y en el Capítulo V, intitulado: "*De la violación de Secretos y comunicaciones*", se erigieron dos tipos penales básicos (Violación ilícita de comunicaciones y Divulgación y empleo de documentos reservados, artículos 228 y 229), con sus correspondientes tipos penales agravados, para proteger las comunicaciones, la confidencialidad de las mismas, el contenido (elemento ideológico de las comunicaciones) y por supuesto, el secreto que generan dichas comunicaciones.

Para aquél entonces se contaba con el artículo 38 de la Constitución de 1886, como fundamento constitucional de la protección de las comunicaciones, con el siguiente tenor: "La Correspondencia confiada a los telégrafos y correos es inviolable. Las cartas y papeles privados no podrán ser interceptados ni registrados sino por autoridad, mediante orden de funcionario competente, en los casos y con las formalidades que establezca la ley y con el único objeto de buscar pruebas judiciales". Agregaba el inciso 2º, "Para la tasación de impuestos y para los casos de intervención del Estado, podrá exigirse la presentación de los libros de contabilidad y demás papeles anexos". El Inciso 3º, finalizaba diciendo: "Podrá gravarse, pero nunca prohibirse en tiempos de paz, la circulación de impresos por los correos".

El término correspondencia utilizado por la Constitución, aunque lo hace en forma genérica para "telégrafos" y "correos" (sinónimo de correspondencia), aquella hace referencia sólo a las "cartas que se despachan o reciben" en forma manual, manuscrita o mecanografiada, según el diccionario, aunque bien es cierto, tanto la cartas, los telegramas, o despachos transmitidos a distancia (telégrafo eléctrico o telégrafo óptico), son medios idóneos para enviar y recibir informaciones, datos o mensajes de texto o vía eléctrica u óptica y en este sentido entonces, todos estos medios apuntaría a enviar y recibir mensajes.

Es apenas obvio, que para la época en que surgió la Constitución las anteriores eran las formas tradicionales de correspondencia y por eso, la Constitución se refería en concreto a las cartas, a los telegramas y a los "papeles privados" enviados y recibidos entre las personas como objeto de protección constitucional y sobre todo de inviolabilidad. Desde aquella época se podría plantear que lo que protegía la Constitución era tanto el objeto material (la carta, el telegrama o papeles) como el contenido de aquellas, es decir, del mensaje, las informaciones o datos contenidos en aquellas. En efecto, hay que hacer dicha aclaración, porque no sólo se

protege el objeto, sus sellos, su lacrado o cerrado (parte externa de la carta), sino el contenido mismo: los mensajes, datos o informaciones que contiene y que subjetivaban la comunicación entre las personas mencionadas como remitente y remitido.

La extinguida Constitución imponía como principio general desde aquél entonces que toda clase de correspondencia entre particulares es inviolable y por tanto, no podría ser intervenida ni registrada, salvo en los casos que la ley y autoridad competente lo requieran como pruebas judiciales. Esta era la única excepción que se planteaba a la inviolabilidad de las comunicaciones oficiales o privadas, y por eso, el legislador penal de 1980, previos los anteproyectos de 1974, 1978 y 1979, estimó conveniente proteger penalmente las comunicaciones entre particulares y entre éstos con los funcionarios del Estado o bien entre funcionarios del Estado, cuando se desborde el texto constitucional en su regla general y excepción correspondiente.

5.1. DELITO DE VIOLACION ILICITA DE COMUNICACIONES.

5.1.1. Tipo penal. El Artículo 288, sostenía: "*El que ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida una comunicación privada dirigida a una persona o se entere indebidamente de su contenido, incurrirá en arresto de seis meses a dos años, siempre que el hecho no constituya delito sancionado con pena mayor.*

La pena será de ocho meses a tres años de arresto si se tratare de comunicación oficial.

Si el autor del hecho revela el contenido de las comunicaciones, o la emplea en provecho propio o ajeno o con perjuicio de otro, la pena será de prisión de uno a tres años, si se tratare de comunicación privada, y de dos a cinco años si fuere oficial".

5.1.2. Fuente Normativa: Art. 228 C.P., de 1980. Derogado por la Ley 599 de 2000 o Código Penal vigente.

5.1.3. Sujeto Activo: Sin calificación alguna. Lo cual quiere decir, que puede cometer el delito tanto los particulares como los empleados públicos, pero en éste último caso se aplicaría el delito más grave por su connotación y cualificación especial de empleado del Estado.

5.1.4. Ubicación en el Código Penal: Los tipos penales básicos y agravados se hallan ubicados en el Titulo X. "Delitos contra la Libertad Individual y otras garantías" y en **Capítulo V,** relativo a la **"Violación de Secretos y Comunicaciones".**

5.1.5. Comunicación privada y oficial. La norma penal a diferencia de la Constitución, se refirió específicamente a "comunicación privada" y "comunicación oficial", para englobar toda clase de comunicaciones existente entre las personas, desde las simplemente manuales hasta las que utilizan medios tecnológicos. Sin embargo, como hace notar el tratadista *Pérez* **[40]**, "las comunicaciones son todas las que el hombre emplea para transmitir su pensamiento…, pues observa *Maggiore*, las cartas propiamente dichas, las esquelas, tarjetas postales, tarjetas de visita contentivas de algún mensaje, las transmisiones telegráficas, los billetes urgentes de servicio y las notas de pedidos de libros… Se incluyen los *pliegos,* o sea, toda carta que exceda del peso prescrito, y todo conjunto de cartas. No se consideran de esta naturaleza los paquetes postales, giros, manuscritos e impresos que no contengan mensajes epistolares, así como las muestras y otros envíos similares".

Agrega el tratadista citado: “En la correspondencia telegráfica se comprende la *hoja* que contiene el despacho o que el remitente ha hecho escribir, o que ha sido recibido o copiado por el empleado receptor o impreso mecánica o eléctricamente”.

5.1.6. La Intimidad en las comunicaciones. Ya comentábamos antes que la fenecida Constitución de 1886, establecía la “inviolabilidad” de toda clase de “correspondencia” entre las personas y que no solo se extendía al objeto material contentivo de los mensajes, sino a éstos mismos, pues no se entiende lo uno sin lo otro. Sin embargo, el pe*nalista Pérez* **[41],** comenta en su obra que no faltaron quienes sostenían que al erigir como delitos la inviolabilidad de la correspondencia en el Código Penal, debería protegerse la propiedad de las cartas y por lo tanto tuteladas bajo el bien jurídico del Patrimonio Económico. Otros por el contrario, manifestaban que debía protegerse el derecho de autor de quien elabora la carta o remitente y “los que lo discernían al destinatario de las comunicaciones”.

El penalista *Pérez* **[42]**, citando a Linares Quintana, distingue tres grados diversos de respeto de la correspondencia epistolar: a) El derecho de la propiedad material, que pertenece al destinatario; b) El de la propiedad intelectual, que eventualmente puede corresponder a quien la remite, cuando la carta o el escrito contiene una obra de ingenio, de valor científico o literario; y c) el derecho al secreto de la correspondencia, que pertenece tanto al remitente como al destinatario. Concluye el penalista *Pérez*, que a éste tercer grado de tutela al que se refiere el texto constitucional (art.38). Sin embargo, creemos que al derecho al sigilo o secreto de la correspondencia más se refieren los artículos 288 y 289 del Código Penal del 80, cuando hace mención a la protección del “contenido” de la correspondencia que no se puede enterar “indebidamente” persona alguna o que no puede ser divulgado o empleado su contenido, para sacar provecho propio o ajeno, o causar perjuicio a otro.

Es aquí donde se vulnera la confidencialidad, integralidad y disponibilidad del derecho de secreto o sigilo en la correspondencia y consecuentemente donde se desconoce una de las esferas de la intimidad, es decir, los mensajes, los datos, las informaciones personales contenidas en la comunicación interpersonal y por eso se ha dado en llamar la “intimidad en las comunicaciones”.

5.1.7. Verbos alternativos para el tipo penal básico. Existen varios verbos alternativos y concurrentes que configuran el tipo penal básico de “*Violación ilícita de las comunicaciones*”. Estos son: (i) ***sustraer***, despojar, quitar, hurtar una comunicación dirigida a una persona por otro; (ii) ***ocultar,*** esconder, encubrir, velar una comunicación para que no se la reconozca de sus elementos exteriores o interiores, según el tipo de comunicación p. el remitente; (iii) ***extraviar***, perder, desviar, traspapelar una comunicación para que no llegue a su destino; (iv) ***destruir***, arruinar, devastar, demoler una comunicación para que sea irreconocible en sus datos de remitente y destinatario, y “esto se logra rompiéndolos, de manera que no pueda ser reconstruidos, quemándolos, disolviéndolos por cualquier procedimiento eliminatorio” **[43]** ; (v) ***Interceptar,*** impedir, obstaculizar, entorpecer, obstruir una comunicación, previa apropiación antes de que lleguen a su destinatario, pues el “*interceptor está colocado entre el remitente y la persona a quien se dirige el envío, y su conducta consiste en dificultar el entendimiento entre los dos. La interceptación comprende las otras actividades: la correspondencia puede interceptarse para su extravío, destrucción o apoderamiento*” **[44]** .; (vi) ***Controlar,*** inspeccionar, vigilar, registrar o examinar una comunicación. “*Las controla quien la somete a su voluntad, a fin de que no lleguen en tiempo oportuno, para que lleguen unas y después otras, o para que regresen al lugar donde se introdujeron, con cualquier pretexto, verbigracia, falta de dirección…*”**[45]**; (vii) ***Impedir,*** frenar o paralizar una comunicación. “*Impide las comunicaciones*

---

(40) PEREZ, Luis C. ***Derecho Penal.*** Parte General y Especial. Tomo IV, Editorial Temis, Bogotá, p. 437 y ss.
(41) a (45) PEREZ, Ob ut supra cit. 437

quien no permite que se transmitan o que se envíen, por ejemplo, dañando los vehículos en que se transportan…", (viii) Enterarse indebidamente de su contenido. Aunque la acción de enterarse del contenido de una comunicación se halla inmersa en el verbo rector "Controlar", pues como se dijo tiene como sinónimos inspeccionar, registra o examinar una comunicación, el legislador del 80, reglamentó separada y alternativamente la acción de enterarse del contenido de dicha comunicación.

El tratadista cita sostiene que "*enterarse indebidamente del contenido de una comunicación es conocerlo sin derecho a ello, es decir, sin cumplir las formalidades prescritas por la ley para violar la intimidad o el secreto de los envíos o de las transmisiones*" **[46]**

5.1.8. Tres (3) tipos penales agravados del tipo básico de "Violación de Comunicaciones" del artículo 288 C.P. Son: (i) Si las acciones del tipo penal básico se realizan con comunicaciones oficiales (Inciso 2º del art. 288 ibíd.); (ii) Indiscreción o "revelación" del contenido de comunicaciones públicas y privadas; y, (iii) Uso o empleo de las comunicaciones en provecho propio o ajeno o con perjuicio de otro.

En el segundo y tercer tipo penal agravado, debe distinguirse si se trata de comunicación de carácter privado o de carácter oficial, pues la pena se agrava aún más si se trata de comunicación oficial.

Revelar es "descubrir o manifestar lo ignorado o secreto", según el diccionario, sin más aclaraciones que quien revela debe ser una persona ajena o distinta a la que ha creado el mensaje o la persona a la que le ha llegado el mensaje. Sin embargo, el penalista ut supra citado, agrega que debe aclararse el verbo revelar que trae el artículo 288 del verbo divulgar mencionado en el artículo 289, porque los efectos jurídicos de una y otra conceptualización en los tipos penales que trae el C.P., del 80, son diferentes, pues el término revelar "*no es tan trascendente como el de divulgar… revelar es particular el secreto, manifestarlo a otros, descubrirlo sin mayores alcances, aunque después se amplíen , y se refiere a las comunicaciones de cualquier clase…"* **[47]**.

5.2. DELITO DE DIVULGACIÓN O EMPLEO DEL CONTENIDO DE LA COMUNICACIÓN PÚBLICA O PRIVADA.

5.2.1. Tipo penal. El artículo 289, sostenía: "*El que en provecho propio o ajeno con perjuicio de otro divulgue o emplee el contenido de un documento que deba permanecer en reserva, incurrirá en arresto de seis meses a dos años, siempre que el hecho no constituya delito sancionado con pena mayor"*.

5.2.2. Fuente Normativa: Artículo 228 del C.P de 1980, derogado por la Ley 559/00.

5.2.3. Sujeto Activo: Sin calificación alguna. "El que" sin calificativo, significa que el sujeto activo del ilícito puede ser un particular o empleado público. Sin embargo, si el delito lo comete un empleado público, se aplicarán los artículos 154 y 155 del C.P., del 80, por contener penas más graves a esta clase de sujetos y por cuanto le son tipos penales específicos aplicables a ellos

5.2.4. Ubicación: Tipo penal básico de *divulgación o indiscreción de la comunicaciones que deben permanecer en reserva* (Se excluyen los documentos públicos por su naturaleza, salvo

---

(46) PEREZ, Ob ut supra cit. 437
(47) PEREZ, Ob ut supra cit. 445

la excepciones de ley) se encuentra en el Titulo X. *Delitos contra la Libertad Individual y otras garantías*. **Cap. V.** *"Violación de Secretos y Comunicaciones"***.**

A este tipo penal le son aplicables los conceptos generales de correspondencia, comunicación privada y pública y los aspectos de invasión, apropiación y revelación del contenido de la comunicación realizada en el aparte anterior.

5.2.5. Conceptualización. El tipo penal, comentado utiliza la expresión "*el contenido de un documento que deba permanecer en reserva*", con lo cual los atentados contra dichos documentos se concentra en el contenido, es decir, en la parte esencial o ideológica del contenido, en aquella parte que significa el derecho de autoría de quien realiza un documento. Sin embargo y de conformidad por el tratadista Linares citado por el penalista colombiano Pérez, debemos decir, que es sobre el contenido mismo de la comunicación donde el Estado ejerce su tutela, al menos en este tipo penal en específico, puesto que aquí se halla el secreto del mensaje y la confidencialidad del mismo que debe permanecer "en reserva". Por tanto, conviene aclarar la conceptualización de documento empleada por el tipo y si le es aplicable el concepto que trae el Código Penal del 80, para los delitos de falsedad y extensible a todos los tipos penales en el artículo 219 y ss., y artículo 225.

Según el artículo 255, sobre el título "Otros Documentos", el Código Penal sostiene: "*Para efecto de los artículos anteriores se asimilan a documentos, siempre que puedan servir de prueba, las expresiones de persona conocida o conocible recogidas por cualquier medio mecánico, los planos, dibujos, cuadros, fotografías, cintas cinematográficas, radiográficas, fono-ópticas, archivos electromagnéticos y registro técnico impreso*".

En principio el penalista *Pérez* [48], sostiene que no es aplicable por que la conceptualización está dada para los delitos de falsedad donde están ubicados el artículo 219 (falsedad ideológica en documento público) y 225, "*materia no contemplada en el artículo 289*". Más aún, se dice que el término "Documento" fue cuestionado desde la redacción del C.P. del 80, pues debió decir "escritos" secretos ya que se refería a objetos materiales o mensajes contenidos en éstos --y no necesariamente a "documentos", entendidos como tales-- que podrían atentar la privacidad o intimidad de las personas tales, como cartas, postales, escritos que contengan obligaciones civiles o comerciales: testamentos cerrados o asuntos familiares, negocios, promesas, apuestas, uniones o separaciones íntimas, etc. Pese a todo, el artículo 289, quedó redactado con el término "documentos" y por tanto deberá estarse a los efectos de conceptualizar documento, lo que sobre el particular se menciona en el artículo 255, por no existir otra norma referida a éstos en la parte general del Código Penal.

5.2.6. Verbos Rectores Alternativos del tipo penal: Son ***Divulgar o emplear*****.** Aunque es discutible, lo plasmado por el tratadista Pérez [49] **,** al decir, que el verbo revelar utilizado en el inciso 3º del artículo 288 del C.P., difiere del verbo "divulgar" utilizado en el inciso único del artículo 289 del C.P., porque son acciones humanas diversas para la construcción del tipo penal, pues revelar tiene unas connotaciones de descubrir, manifestar o participar un secreto a otra persona, sin más; y que divulgar "equivale a publicar, difundir o extender considerablemente las conversaciones escritas", indicando con ello, que la divulgación es más extendida y por diversos mecanismos que revelar que resulta menos extendida.

5.2.7. Elementos constitutivos del ilícito: "en provecho propio o ajeno" y "con perjuicio de otro". Estos elementos antes que ser constitutivos de un ilícito, son agravantes del mismo, tal como se puede observar en los tipos agravados del artículo 288, Inciso 3º. Sin embargo,

---

(48), (49) PEREZ, Ob ut supra cit. 445

aquí se utilizan como elementos que estructuran el delito pero anteponiendo estos apelativos agravantes al tipo penal de divulgación y empleo del contenido del documento que "debe permanecer en reserva". Siendo esto último lo más grave de la configuración del ilícito que puede ser objeto de vulneración por el agente.

6. LA INTIMIDAD COMO BIEN JURIDICO TUTELADO EN EL CODIGO PENAL DEL 2000

6.1. LA INTIMIDAD QUE TUTELA EL CÓDIGO PENAL DEL 2000

Hemos dicho que la intimidad de las personas al ser elevada a rango constitucional en el derecho colombiano, lo hizo basado en la concepción universal y regional que aquella tiene en los actuales momentos no sin recoger la conceptualización evolutiva que la intimidad tiene desde aquel ensayo jurídico norteamericano de *Warren* y *Brandeis*, sobre "*The right to privacy*" de 1890, con facultades de derecho a no ser molestado por nadie en su recinto domiciliario o sitios asimilables a éste y de control de la imagen de las personas por terceros que sin autorización o consentimiento de aquél las publican o utilizan como material periodístico.

En efecto, hoy la intimidad como derecho fundamental, autónomo pero limitado por los derechos y libertades de los demás, el no abuso del propio derecho y por el ordenamiento jurídico vigente, presenta varias facetas o visiones que lo estructuran productos de esa evolución.

Por estas múltiples facetas o visiones y su permeabilidad o conflicto con otros derechos y libertades fundamentales se dice que la intimidad con bien jurídico protegido es de carácter *difuso* [50]. Algunas de esas visiones son:

(i) La visión primigenia de la intimidad. La protección a la vida "privacy" o la vida privada de las personas contra todo atentado a la vida íntima en su casa, sus pensamientos, ideas, sentimientos, acciones hacia el interior de su hogar, al derecho a la soledad pacífica y sin injerencias ajenas. Visión original y típica de la intimidad;

(ii) La visión de autocontrol de la imagen de la persona y de la circulación o publicación de la misma inicialmente por medios fotográficos tradicionales y con el tiempo y evolución tecnológica por reproducciones digitales, virtuales, computarizadas o a través de telecomunicaciones por vías telemáticas;

(iii) La visión domiciliaria de la intimidad (extensión de la originaria visión del *My home is my castle*). La cual se extiende;

(iv) La visión corporal de la intimidad (extensión de la visión de autocontrol de la propia imagen), que comprende no sólo la parte física o morfológica de la persona: su caracterización personal y sus rasgos estructurales únicos (color de piel, cabello, ojo, etc.) deformidades (Cara, extremidades superiores o inferiores, estatura, etc.) o exaltaciones físicas propias de cada ser humano; sino las de índole corporal interno, como los líquidos humanos: sangre, semen, orina, sudor, etc.; enfermedades genéticas, hereditarias o adquiridas; entre otros muchos aspectos;

---

(50) ROMBO CASABONA, Carlos María. ***Los datos de carácter personal como bienes jurídicos penalmente protegidos.*** En: AA.VV. El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales. Estudios de Derecho Penal y criminología, Editorial Comares S.L., Granada, 2006, p. 166 y ss.

(v) La visión ideológica de las comunicaciones en cualquiera de sus formas: tradicionales o escritas (cartas, postales, papeles, etc.), o bien utilizando medios TIC e informática (teléfono, telefax, mensajes de correo electrónico, Chat, teleconferencia, etc. o bien usando la telemática: video, sonido e imagen). Esto es lo que se conoce como la Intimidad en las comunicaciones;

(vi) La visión internacionalista americana de la intimidad contra toda injerencia arbitraria, abusiva o ilegal de la vida privada, su familia y su correspondencia, según la Declaración de Derechos Humanos de la ONU, los Tratados de Derechos civiles y políticos de San José de Costa Rica y de New York, ratificados por Colombia en leyes 74 de 1968 y 16 de 1972;

(vii) La visión internacionalista europea de la intimidad, sobre recolección, almacenamiento, registro, reforma, actualización, cancelación, circulación o transmisión y acceso de datos personales "automatizados o no" y su tratamiento o procesamiento en bases de datos o ficheros y sus correspondientes derechos de oposición al acceso, la interceptación y transmisión sin consentimiento del concernido o autorización judicial por medios tradicionales o por medios TIC e informática. Visión prevista en el Convenio de Europa de 1980 y las Directivas Europeas 95/46/CE y 97/66/CE. Visión que se recoge en las legislaciones internas de cada Estado miembro de la UE. España, p.e. en la LORTAD de 1992 y la LOPDP o Ley 15 de 1999, Ley Orgánica de protección de datos personales;

(vii) La visión ius-informática de la intimidad, consistente en la información personal o datos de la persona humana, que como unidades de información se hallan recolectadas, tratadas, transmitidas y difundidas por medios informáticos, electrónicos o telemáticos, bien se hallen en bases de datos o ficheros públicos o privados; o bien se procesen o circulen entre redes internas (intranet) o externas (Internet) como registros individuales de información. En esta visión propuesta por nosotros [51] , se potencia la protección jurídica del Estado y los mismos particulares de la información, los datos o unidades de información recogida, procesada o transferida por medios TIC y la informática. Las facultades principales en esta visión de la intimidad son: el autocontrol de la información que le concierne a una persona en todo el procesamiento informático desde la recolección de la información hasta su circulación, flujo o transmisión de la misma; y, la utilización de todos los mecanismos jurídico materiales y procesales para oponerse un procesamiento informático en el cual no haya precedido el consentimiento del titular de la información, o no haya autorización judicial para hacerlo. Los mecanismos de oposición inicialmente son iuscivilistas, administrativistas y como última ratio, los de índole contravencional y penal.

En este panorama que no *numerus clausus,* como se anotó al conceptualizar la Intimidad y su evolución, observamos que el Código Penal del 2000, instituyó como bien jurídico tutelado explícito a la intimidad en la visión ideológica de las Comunicaciones (artículos 192 a 197) y en forma tácita, aunque bajo otro bien jurídico tutelado ("la información y los datos" personales), la visión ius-informática de la intimidad en los artículos 269 A a 269 J. Igual sucede con otras visiones de la intimidad que previamente al C.P., del 2000, ya se hallaban reguladas en diversos tipos penales y bajo otros bienes tutelados. V.gr. Delitos contra la inviolabilidad de domicilio o de sitio de trabajo. Los cuales tenían que ver con la "intimidad domiciliaria". Eso prueba el carácter difuso de la intimidad aunque hoy se viene abriendo una tesis internacionalista europea en la cual se dice que del derecho a la intimidad se "desgajan" otros "nuevos derechos fundamentales", como el de "protección de los datos personales",

---

(51) RIASCOS GOMEZ, Libardo O. ***El derecho a la intimidad, su visión ius-informática y los delitos relativos a los datos personales.*** Tesis doctoral, Universidad de Lleida (España), 1999, pág. 320 y ss

estructurado como lo expone *Rombo Casabona* [52], de las previsiones del artículo 18.4 de la CE, que impone la limitación de la informática en el tratamiento de datos personales, los contenidos de las leyes internas que reglamentan los datos personales (La LOPDP de 1999) y las normas europeas (Directivas del Consejo de Europa, antes citadas), sobre protección de los derechos de la intimidad, honor e imagen de los datos personales en la circulación, movimiento internacional o flujo de datos transfronterizo.

En Colombia siguiendo los parámetros de las normas internacionales americanas ut supra citadas y como veremos más adelante, hablamos de un nuevo derecho fundamental: el "Habeas Data" [53] que consiste en el derecho que tiene toda persona para solicitar de cualquier autoridad estatal o particular, la actualización, rectificación o eliminación de los datos personales que le conciernen si ya se han almacenado en bases de datos o ficheros, cualquiera sea los fines y objetivos de éste, con o sin su consentimiento; o bien ejercer los derechos de oposición (administrativa o jurisdiccional) a la recolección, almacenamiento, difusión o transmisión de los datos personales de su titularidad, si vulneran otros derechos como la intimidad, el honor, la imagen o la libertad individual o el libre desarrollo de la personalidad. Sobre este nuevo bien jurídico protegido haremos mención *ut supra*.

6.2. TIPOS PENALES CONTRA LA INTIMIDAD EN LAS COMUNICACIONES

6.2.1. Las comunicaciones en el Código Penal del 2000

El Código Penal del 2000, al igual que lo hiciera el C.P., del 80, instituyó como bien jurídico protegido la reserva e interceptación de las comunicaciones, pero adicionada la intimidad dentro de dicho bien jurídico. En consecuencia, hoy por hoy, tenemos como bien jurídico protegido en el Capítulo VII del Titulo X de los delitos contra la Libertad individual y otras garantías del C.P., vigente, a la intimidad y el secreto e interceptación de la comunicaciones, o dicho de otro modo, la intimidad en las comunicaciones cualquiera sea la forma, tipo y medio manual, eléctrico, electrónico, informático o telemático en el que se realice, pues el intitulado del bien jurídico protegido como el contenido normativo del mismo no hizo salvedades ni aclaraciones de ningún tipo.

La Constitución del 1991 en el inciso 3º del artículo 15, manifestó que "*la correspondencia y demás formas de comunicación privada son inviolables. Solo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley*". Con ello, reconoce que además de la correspondencia, es decir, aquella comunicación escrita que se envía y recibe por las personas, existen otras "*formas de comunicación privada*", escritas como las cartas o misivas, "papeles" que contengan mensajes entre personas, tarjetas postales, esquelas, tarjetas de visita contentivas de algún mensaje, los "pliegos", o sea "toda carta que exceda del peso prescrito" y todo conjunto de cartas. No se considerarán comunicaciones escritas manuales, los paquetes postales, giros, manuscritos e impresos "que no contengan mensajes epistolares", así como las muestras y otros envíos similares, según lo observa *Maggiore* citado por el penalista *Pérez* [54] .

Son comunicaciones que utilizan medios eléctricos por ejemplo, el telégrafo (sin hilos) que es el aparato "eléctrico en que las señales se transmiten por medio de las ondas hercianas, sin necesidad de conductores entre una estación y otra", y su correspondiente telegrama o sea, el "*papel normalizado en que se recibe escrito el mensaje telegráfico*", aunque hoy uno y otro

---

(52) ROMBO CASABONA, Carlos María. ***Ob., ut supra cit.,*** *p. 169*

(53) RIASCOS GOMEZ, Libardo O. ***El habeas Data: Visión constitucional, visión legal y en proyectos de Ley Estatutraria.*** En http://akane.udenar.edu.co/derechopublico

(54) Ob ut supra cit., p.439.

sean de poca usanza.

Constituye una comunicación vía electrónica el denominado "fax" que proviene de la abreviatura de la voz inglesa "facsímile" y consiste en un "*sistema que permite transmitir a distancia por la línea telefónica escritos o gráficos*".

La comunicación verbal entre las personas también puede considerarse en este aparte, pues mientras haya quien diga algo (emisor), que se dice (mensaje), por qué medios (canales, en este caso la voz), y a quién se dice (receptor) y qué efecto se produce (información de retorno al emisor), estaremos ante un proceso de comunicación básico y humano [55]. Si se rompe, interrumpe, suspende o intercepta este proceso de comunicación se produce una actuación como mínimo inapropiada con efectos jurídicos teniendo en cuenta la connotación y contenido del mensaje, como veremos *ut infra.*

La comunicación vía teléfono fijo o móvil y todas las que se derivan de aquellos en las denominadas nuevas tecnologías de la información y la Comunicación, TIC, que emplean un "*conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios, que permiten la compilación, procesamiento, almacenamiento, transmisión de información como voz, datos, texto, video e imágenes*" (art. 6º de la Ley 1341 de Julio 30 de 2009, "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones —TIC—, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones").

6.2.2. Tipos penales básicos y agravados

Los tipos penales básicos y agravados contra la intimidad de las comunicaciones están previstas en los artículos 192 a 196 del Código Penal de 2000, reformado parcialmente y que afecta a los subsiguientes tipos: La Ley 890 de 2004 por la cual se modifica y adiciona el Código Penal; Ley 1142 de 2007 "*Por medio de la cual se reforman parcialmente las Leyes 906 de 2004, 599 de 2000 y 600 de 2000 y se adoptan medidas para la prevención y represión de la actividad delictiva de especial impacto para la convivencia y seguridad ciudadana"* y Ley 1288 de 2009 "*por medio del cual se expiden normas para fortalecer el marco legal que permite a los organismos, que llevan a cabo actividades de inteligencia y contrainteligencia, cumplir con su misión constitucional y legal, y se dictan otras disposiciones*". Estos son:

1) Violación ilícita de comunicaciones privadas (Artículo 192)

En el primer inciso del artículo 192 se encuentran dos tipos penales básicos, (i) la primera parte de este tipo penal doctrinalmente se conoce como *control audiovisual clandestino y control ilícito de señales de comunicación*, por los medios de comunicación utilizados (tradicionales y TIC e informática) y los verbos rectores (sustraer, ocultar, extraviar, destruir, interceptar, controlar e impedir); (ii) La segunda parte del tipo, constituye un *delito de descubrimiento ideológico o del contenido de las comunicaciones*, pues lo determinante en este aparte es que el agente se "entere indebidamente de su contenido" referido a las comunicaciones privadas.

En el segundo inciso del mentado artículo se hallan dos tipos penales agravados de la violación ilícita de comunicaciones privadas, a saber: (i) Delito de Revelación ideológica o del contenido de la comunicación; (ii) Delito empleo en provecho propio o ajeno o con perjuicio de

---

(55) **RIASCOS GOMEZ, Libardo O.** ***La Constitución de 1991 y la informática jurídica.*** Editorial UNED, Universidad de Nariño, Pasto, 1997, p. 3.

otro de la violación de las comunicaciones privadas. Este tipo agravado es alternativo y se configura con la comisión de una de las tres posibilidades.

2) Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas (Artículo 193)

En este se encuentra un único tipo penal básico con varios verbos alternativos para su estructuración, conocido como *negociación ilícita de instrumentos idóneos para la interceptación de comunicaciones privadas.*

3) Divulgación y empleo de documentos reservados (Artículo194). Aquí ubicamos un solo tipo penal básico, con verbos alternativos (divulgar o emplear el contenido de un documento que debe permanecer en reserva) con fines determinantes del tipo diferentes: (i) En provecho propio o ajeno; y, (ii) Con perjuicio de otro.

4) Violación ilícita de comunicaciones o correspondencia de carácter oficial (Artículo 196). Ubicamos un tipo penal básico de violación ilícita de comunicaciones de carácter oficial, conocido doctrinalmente como delito de *control audiovisual clandestino y control ilícito de señales de comunicación de carácter oficial*, por los medios de comunicación utilizados (tradicionales: correspondencia escrita o telegráfica y por medios TIC e informática) y los verbos rectores (sustraer, ocultar, extraviar, destruir, interceptar, controlar e impedir). En el segundo inciso del artículo se halla un tipo penal agravado de la violación ilícita de comunicaciones oficiales, cuando: (i) se comete contra comunicación o correspondencia oficial dirigida a las dependencias o autoridades de la rama jurisdiccional o los organismos de control (Contraloría, Procuraduría y Defensoría del Pueblo y todos los organismos y dependencias que los componen a nivel nacional, departamental, distrital o municipal), como a los organismos y dependencias de Seguridad del Estado (Fuerzas Armadas y Policía, etc.).

6.2.2.1. Delito de Violación Ilícita de comunicaciones

6.2.2.1.1. Fuente normativa: Art.192 C.P., reformado parcialmente por la (i) Ley 890 de 2004, artículo 14, en cuanto aumento de penas; (ii) La Ley 1341 de 2009, sobre la conceptualización de los nuevos medios de la información y la comunicación o TIC, régimen jurídico de la telefonía fija y móvil e infracciones contravencionales que afectan al derecho de la intimidad, el honor y demás libertades y derechos constitucionales cuando existen actuaciones ilícitas en las comunicaciones; (iii) El Decreto 075 de 2006, *Por medio del cual se definen las obligaciones que le asisten a los operadores de servicios de telecomunicaciones en procura de optimizar la labor de investigación de los delitos por parte de las autoridades competentes".* La Fiscalía General de la Nación es el organismo del Estado encargado de la coordinación con los organismos con funciones de Policía Judicial, del manejo de las actividades y procesos relacionados con la interceptación de los servicios de telecomunicaciones; (iv) El Artículo 235 C.P.P [56], reformado por la Ley 1142 de 2007,

---

(56) ***Artículo 235. Interceptación de comunicaciones telefónicas y similares***. El fiscal podrá ordenar, con el objeto de buscar elementos materiales probatorios, evidencia física, búsqueda y ubicación de imputados o indiciados, que se intercepten mediante grabación magnetofónica o similares las comunicaciones telefónicas, radiotelefónicas y similares que utilicen el espectro electromagnético, cuya información tengan interés para los fines de la actuación. En este sentido, las entidades encargadas de la operación técnica de la respectiva interceptación tienen la obligación de realizarla inmediatamente después de la notificación de la orden./ En todo caso, deberá fundamentarse por escrito. Las personas que participen en estas diligencias se obligan a guardar la debida reserva./ Por ningún motivo se podrán interceptar las comunicaciones del defensor./ La orden tendrá una vigencia máxima de tres (3) meses, pero podrá prorrogarse hasta por otro tanto si, a juicio del fiscal, subsisten los motivos fundados que la originaron.

reglamenta el procedimiento de interceptación de las comunicaciones telefónicas y similares, realizadas por la Fiscalía mediante la grabación magnetofónica o similares y el artículo 237 Id[57], sobre audiencia de control de legalidad posterior sobre la interceptación, por parte del juez de control de garantías.

6.2.2.1.2. Tipo delictivo: "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 dieciséis (16) a cincuenta y cuatro (54) meses, 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 treinta y dos (32) a setenta y dos (72) meses.

6.2.2.1.3. Ubicación en el C.P.: Titulo X, De los Delitos contra la Libertad Individual y otras Garantías, **Capítulo VII:** *Violación a la intimidad, reserva e interceptación de comunicaciones*.

El Capítulo VII del C.P., del 2000, se diferencia del Capítulo VII del C.P., del 80, en que éste último no consideraba expresamente el bien jurídico protegido de la intimidad, como sí lo hace el vigente Código Penal, el cual abarca a los cuatro tipos penales básicos y los tipos agravados. El tipo penal de violación ilícita de las comunicaciones de carácter privado involucra esa faceta de la intimidad referida a la inviolabilidad de todo tipo de comunicaciones orales, eléctricas, electrónicas, informáticas y telemáticas. Con este actuar se ha logrado dotar al tratamiento penal de la tutela de la intimidad y una unidad y coherencia sistemática de la que carecía el Código Penal del 80.

Sin embargo, el bien jurídico protegido de la intimidad, no atrajo a éste capítulo ni lo atinente a los ilícitos cometidos contra la reserva del "secreto profesional", ni los delitos contra la inviolabilidad de morada o habitación ajena y similares que suponen la visión de la intimidad domiciliaria y que perfectamente podría haber quedado cobijados bajo este bien tutelado, como sucede en el derecho penal español [58].

6.2.2.1.4. Sujeto Activo: Al utilizar el tipo penal la expresión "El que" para referirse a la persona que puede ser el agente de la comisión del delito, lo hace en forma general, sin calificación alguna, con lo cual se entiende que puede cometer el ilícito un particular o un servidor del Estado (De carrera, libre nombramiento y remoción, de elección popular, de contrato, de período o de vinculación estatutaria). No existe tipo penal alguno que agrave las sanciones penales cuando el sujeto activo sea un servidor estatal, como sí existe en otros tipos penales, esto por cuanto el nivel de insidiosidad delictiva de parte de este tipo de

---

(57) ***Audiencia de control de legalidad posterior.*** Dentro de las veinticuatro (24) horas siguientes al cumplimiento de las órdenes de registro y allanamiento, retención de correspondencia, interceptación de comunicaciones o recuperación de información dejada al navegar por Internet u otros medios similares, el fiscal comparecerá ante el juez de control de garantías, para que realice la audiencia de revisión de legalidad sobre lo actuado, incluida la orden./ Durante el trámite de la audiencia sólo podrán asistir, además del fiscal, los funcionarios de la policía judicial y los testigos o peritos que prestaron declaraciones juradas con el fin de obtener la orden respectiva, o que intervinieron en la diligencia./ El juez podrá, si lo estima conveniente, interrogar directamente a los comparecientes y, después de escuchar los argumentos del fiscal, decidirá de plano sobre la validez del procedimiento./ **Parágrafo.** Si el cumplimiento de la orden ocurrió luego de formulada la imputación, se deberá citar a la audiencia de control de legalidad al imputado y a su defensor para que, si lo desean, puedan realizar el contradictorio. En este último evento, se aplicarán analógicamente, de acuerdo con la naturaleza del acto, las reglas previstas para la audiencia preliminar

(58) MORALES PRATS, *Fermín.* ***Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad de domicilio.*** *Ed. Aranzadi, Pamplona (España), p. 294*

servidores es mayor por sus condiciones y privilegios devenidos de su *status* funcionarial así como el grado de responsabilidad jurídico constitucional y legales devenidos de la función pública (artículos 6, 122,123 y 124 de la Constitución del 91).

6.2.2.1.5. Conceptualización de términos. El término de *"comunicaciones*" utilizado por el artículo 193 del C.P., debe entendérselo a la luz del artículo 15-3, constitucional y las diferentes normas especiales que reglamentan los diversos tipos de comunicación tradicional y devenida de las nuevas tecnologías de información y la comunicación o TIC. En efecto, la norma constitucional se refiere a "la correspondencia y demás formas de comunicación privada" (p.e. "mensajes de correo electrónico"), las cuales son inviolables y no pueden interceptarse, salvo orden judicial y en la forma que determine la ley.

En tal virtud la transmisión de mensajes (orales, auditivos, cifrados, eléctricos o electrónicos) enviados por un emisor hacia un receptor se considera comunicación y ésta puede ser: escrita, verbal, informática, telemática o electrónica (información, datos, imágenes o sonidos).

El artículo 2º de la Ley 527 de 1999 en Colombia conceptualizó lo que se debe entender por mensaje de datos y sistema de información que los engloba, a los efectos de comprender mejor que éstas son nuevas formas de comunicación electrónica y telemática.

Los mensajes de datos en forma electrónico y dentro de éstos, los mensajes de correo electrónico de la siguiente manera: *La información generada, enviada, recibida, almacenada comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (o* EDI. Es La transmisión electrónica de datos de una computadora a otra, que está estructurada bajo normas técnicas convenidas al efecto,*), Internet, el correo electrónico, el telegrama, el télex o el telefax.*

El literal f, del mentado artículo se conceptualiza lo que se entiende por *Sistema de Información**…** (que es) todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.*

En el sistema punitivo colombiano deberá aclararse como lo precisaremos más adelante, que al no prever expresamente el artículo 193 del C.P, la previa aprehensión o apoderamiento del contenido de la comunicación para poder realizar las acciones delictivas alternativas del tipo penal y tratándose de los mensajes de datos deberá interpretarse que las conductas delictivas para que se lleven a cabo podrían darse con "captación mental o intelectual con o sin desplazamiento físico" **[59]**. En el primer caso, se daría la circunstancia con el desplazamiento físico de los mensajes de datos ya impresos y fuera del sistema. Sin desplazamiento físico sería aquellos mensajes de datos que se hallan o leen en la pantalla del computador, por ejemplo.

6.2.2.1.6. Verbos alternativos: Para la constitución del tipo básico penal de violación ilícita de comunicaciones de carácter privado se requiere que la acción humana consista en *Sustraer, ocultar, extraviar, destruir, interceptar, controlar o impedir*. En cambio, para la constitución del tipo penal agravado se requiere una acción de *revelar* el elemento ideológico o de contenido de la comunicación.

Aparentemente para la configuración de los tipos penales básicos y agravados no se requiere el apoderamiento o aprehensibilidad previa de los objetos de comunicación (cartas, postales, mensajes de correo electrónico, etc.) para poder desatar una cualquiera de las subsiguientes acciones del tipo, como sustraer u ocultar, entre otras posibles acciones y así descubrir o vul-

---

(59) MORALES PRATS, *Fermín**. Delitos contra…** Ob., ut supra cit., p. 300*

nerar la intimidad personal o familiar. Sin embargo, debemos entender que dicha aprehender debe darse aunque no con el objeto y fines requeridos para el delito de hurto, sino para que fuese posible el cumplimiento de las acciones de sustraer, despojar o quitar objetos de comunicación, por ejemplo.

El artículo 197 del Código Penal Español, expresamente sostiene la "apropiación" de los "papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales" para ejecutar una acción concomitante o subsiguiente, como la "interceptación (de) telecomunicaciones" o de "utilizar artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o la imagen, o de cualquier otra señal de comunicación".

El penalista *Morales Prats* [60], al respecto explica que *el legislador ha optado por tipificar en un solo precepto los delitos relativos al apoderamiento de documentos o efectos personales con el fin de descubrir la intimidad ajena y los delitos relativos a la interceptación de telecomunicaciones y al control audiovisual clandestino, con un tratamiento punitivo unitario… Esta opción sistemática, anunciada… es discutible. Principalmente, porque desatiende a la diversa insidiosidad que para el bien jurídico intimidad suscita el empleo de un mero apoderamiento físico de documentos o efectos personales frente a la utilización de sofisticados aparatos de control auditivo o visual clandestino; éstos últimos proporcionan un control certero y sistemático, más penetrante que pasa inadvertido para la víctima, lo que debería haberse visto reflejado en un distinto trato punitivo más grave para estos últimos casos.*

6.2.2.1.7. Agravación del delito de Violación Ilícita de comunicaciones. Este tipo básico presenta dos Tipos agravados**,** en el inciso 2º del artículo 192, así: (i) Revelar o difundir: "Delito de indiscreción"; y (ii) Emplear en provecho propio o ajeno o en perjuicio de otro. Se quedó por fuera: Revelar información del núcleo duro de la "privacy" y los de aquellas personas que tienen la condición especial de manejo de los datos, hechos o imágenes, es decir, los Encargados o responsables de bancos de datos, registros o archivos, que en el derecho español tienen mayor penalidad por abarcar un mayor ámbito de insidiosidad punitiva.

En este aparte son válidas las observaciones realizadas al comentar las tipos agravados del artículo 288 del antiguo Código Penal de 1980, pues la redacción del artículo 193 del C.P., del 2000 es idéntica.

6.2.2.2. Delito de Ofrecimiento, Venta o compra de instrumento apto para interceptar la comunicación privada entre personas

6.2.2.2.1. Fuente normativa: Artículo 193 C.P., Ley 1341 de 2009, Tics; El Decreto 075 de 2006 y el 235 CPP, reformado por la Ley 1142 de 2007, sobre Investigación criminal por parte de la Fiscalía General de la Nación y el procedimiento judicial y técnico en ésta clase de telecomunicaciones; La Ley 228 de 1995 estructuró el actual delito previsto en el artículo 194 del C.P., como contravención especial o "contravención penal" de conocimiento en primera instancia de los jueces penales o promiscuos municipales del lugar donde se cometió el hecho, o en su defecto, los del municipio más cercano al mismo e investigadas y juzgadas por un procedimiento especial de audiencias previsto en los artículos 16 a 40 de la citada ley. Dicha contravención tenía una mayor punibilidad que la establecida para el actual delito de idéntica estructuración y redacción penal.

---

(60) MORALES PRATS, *Fermín**. Delitos contra…** Ob., ut supra cit., p. 300*

En efecto, el artículo 14, sostenía: ***Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas.*** *El que sin autorización de la autoridad competente, ofrezca, venda o compre instrumentos aptos para interceptar la comunicación privada entre personas, incurrirá en pena de arresto de seis (6) a dieciocho (18) meses, siempre que la conducta no constituya hecho punible sancionado con pena mayor.* Y agregaba el inciso 2º: *Corresponde al Ministerio de Defensa Nacional impartir las autorizaciones de que trata el presente artículo.*

6.2.2.2.2. Tipo penal. *El que sin permiso de autoridad competente, ofrezca, venda o compre instrumentos aptos para interceptar la comunicación privada entre personas, incurrirá en multa, siempre que la conducta no constituya delito sancionado con pena mayor.*

6.2.2.2.3. Ubicación: Titulo X, De los Delitos contra la Libertad Individual y otras Garantías, Capítulo VII: *Violación a la intimidad, reserva e interceptación de comunicaciones.*

Resulta discutible que el tipo penal previsto en el artículo 193, vulnere la Intimidad, reserva o interceptación de comunicaciones, pues el hecho de la negociación (oferta, compra y venta) de instrumentos aptos para interceptar la comunicación privada entre personas, no es más un acto comercial ilícito de aparatos especiales para la interceptación, sin que nada tenga que ver con la vulneración del bien jurídico protegido, al menos en forma directa e inmediata. Cosa diferente es la persona que los adquiere y los utiliza en la captación intelectual o mental con o sin desplazamiento físico: objetos, datos, correspondencia, cartas, postales, mensajes de datos, etc., pues en este segundo caso es inequívoca las conductas que tienden a vulnerar el bien jurídico protegido y en todo caso se encasillarían el tipo penal previsto en el artículo 192 del C.P., y no en éste.

Ahora bien, si lo que pretendía el legislador del 2000, respecto de este tipo era ubicarlo bajo este bien jurídico tutelado porque se refería a los objetos idóneos con los cuales se llevaba a cabo la interceptación de comunicaciones, pensando más en la sistémica de las comunicaciones que en la de las conductas penales de los agentes de éste tipo de delitos, es relativamente aceptable: 1. Porque el delito de negociación de elementos aptos para las telecomunicaciones, sin que se participe en la ejecución de la conducta, pudiera estar cometiendo un delito de receptación sobre objetos especiales de comunicaciones telegráficas, informáticas, telemáticas o satelitales, según el artículo 447-2 del C.P. (inciso 2º adicionado por el artículo 45 de la Ley 1142 de 2007), con pena mayor que la del actual tipo puesto que puede llegar hasta 13 años de arresto y multa de hasta 700 SMMV y bajo el bien jurídico tutelado del Capítulo VI, sobre *el Encubrimiento*, Titulo XVI, *Delitos contra la eficaz y recta impartición de Justicia.*

2. Porque el negociador de los elementos aptos para la interceptación de comunicaciones o el receptador no realizaría interceptación alguna porque esa no es su finalidad como negociador o receptador, salvo que se iniciara en labor de interceptador ilegal de las comunicaciones apoyado en su conocimiento especializado de los bienes que oferta, vende o compra, caso en el cual habría un concurso de conductas punibles.

La Corte Constitucional C-626-96, sostuvo al respecto que *La comercialización de tales productos sin autorización emanada de autoridad competente lleva implícita la complacencia del oferente o vendedor y la clara intención del comprador en el sentido de hacer uso de los indicados aparatos, que, por sí mismos, están orientados a la práctica de operaciones de interceptación en principio prohibidas por la Carta Política*. Y agrega: *Es evidente que, en cuanto se trata de comportamientos consistentes en ofrecer, promocionar, vender o comprar instrumentos aptos para interceptar las comunicaciones privadas, el bien jurídico protegido no*

es otro que el consagrado, como derecho fundamental, en el artículo 15 de la Constitución Política.

3. La Corte Constitucional en Sentencia C-626-1996, sostuvo la Constitucionalidad y fines protectores de la Intimidad del artículo 14 de la Ley 228 de 1995 en los siguientes términos*: Ninguna persona pública ni privada, por plausible o encomiable que sea el objetivo perseguido, está autorizada para interceptar, escuchar, grabar, difundir ni transcribir las comunicaciones privadas, esto es, las que tienen lugar entre las personas mediante conversación directa, o por la transmisión o registro de mensajes, merced a la utilización de medios técnicos o electrónicos aptos para ello, a menos que exista previa y específica orden judicial y que ella se haya impartido en el curso de procesos, en los casos y con las formalidades que establezca la ley, según los perentorios términos de la Constitución Política.*

6.2.2.2.4. Sujeto Activo: No se requiere cualificación alguna, respecto del agente del delito, por lo que podrá ser un particular o un servidor del Estado. Tampoco tendrá variación alguna respecto de la mayor punibilidad, si las acciones del tipo penal son realizadas por un servidor público, aunque debería haberse hecho la salvedad y creado un tipo penal agravado por la condición del sujeto activo, pues la mayor insidiosidad que puede ocasionar un funcionario público que estuviere habilitado solo para negociar legalmente estos instrumentos aptos para interceptar comunicaciones (pero no para la interceptación misma que depende de la Fiscalía General de la Nación dentro proceso judicial), previa autorización del Ministerio de Defensa Nacional, como rezaba el artículo 14 de la Ley 228 de 1995, su status privilegiado funcionarial y su mayor ámbito de responsabilidad como funcionario del Estado (art. 6 y 122 a 124, constitucionales), lo harían un sujeto en posición conductal potenciada.

Más aún, según la Sentencia C-626-96, *La comercialización de tales productos (aptos para la interceptación) sin autorización emanada de autoridad competente lleva implícita la complacencia del oferente o vendedor y la clara intención del comprador en el sentido de hacer uso de los indicados aparatos, que, por sí mismos, están orientados a la práctica de operaciones de interceptación en principio prohibidas por la Carta Política. resulta natural, y ajustado a la Constitución, que la ley canalice la tenencia y la utilización de los mismos en cabeza de personas y entidades debidamente autorizadas, sobre las cuales se pueda ejercer el control del Estado, de modo que las interceptaciones que en efecto se lleven a cabo provengan invariablemente de orden judicial*.

6.2.2.2.5. Verbos alternativos: Ofrecer, Vender o comprar. La configuración del tipo penal básico se verifica con el cumplimiento de las acciones que pueden ser alternativas. La comercialización o negociación ilícita de los bienes destinados a la interceptación de las comunicaciones telefónicas, telegráficas, informáticas, telemáticas y satelitales, estructura el ilícito previsto en el artículo 193 del C.P. En consecuencia, la negociación lícita de estos elementos de interceptación por personas naturales o jurídicas debida y legalmente autorizadas por el Ministerio de Defensa Nacional, no constituyen delito.

Es claro que el Ministerio de Defensa Nacional es la entidad estatal competente para autorizar la negociación o comercialización a personas naturales o jurídicas de esta clase especial de elementos de interceptación de comunicaciones, pero la interceptación misma para fines judiciales y previa autorización escrita de interceptación cuando se reúna los requisitos legales para hacerla y esté en curso procesos judiciales que lo permitan, corresponde a la Fiscalía General de la Nación de conformidad con el Decreto 075 de 2006, enero 13 y conforme al procedimiento previsto en el artículo 235 del C.P.P.

6.2.2.3. Delito de Divulgación y empleo de documentos reservados

6.2.2.3.1. Fuente normativa: (i) Artículo 194 C.P., (ii) Arts. 46 a 49 Código Nacional de Policía, relativa a las contravenciones especiales contra la "integridad Personal" y que en realidad son contra la Intimidad. ¿Duplicidad de tipificaciones, aún con diferentes formas de conducta punitiva: contravención y delitos?; (iii) Todos tienen derecho de acceso al documento público, salvo los casos previstos en la ley, según el artículo 74, constitucional; (iv) Ley 57 de 1985 o Estatuto de la Información y Documentos Públicos, reformada parcialmente por Ley 594 de 2000, sobre información, Documentos Públicos y archivos en Colombia y la Ley 190/95, normas sobre anticorrupción. Relativas a la Información reservada por espacio de 30 años (artículos 28 y 33, respectivamente).

6.2.2.3.2. Tipo penal. *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.*

Doctrinalmente se le conoce a este ilícito como *delito de descubrimiento o indiscreción de la información reservada contenida en un documento con aprovechamiento*. Este provecho puede ser en interés propio o ajeno, o con perjuicio de otro. El descubrimiento implica no solo la divulgación sino el empleo ideológico de un documento que deba permanecer en reserva.

Tal como está redactado el tipo penal básico de indiscreción parecería más la reiteración de un tipo penal agravado del artículo 192 del C.P., que en un delito autónomo tal como fue concebido por el legislador del 2000. En efecto, hechas las salvedades del caso y comentadas en el delito de violación ilícita de comunicaciones y referidas al tipo agravado de "revelar o difundir el contenido de una comunicación privada entre personas prevista en el inciso 3º del artículo 192 del C.P., sobre (i) la diferencia conceptual de "revelar" y "divulgar"; y, (ii) el elemento ideológico o de contenido del documento; (ii) el empleo de los elementos estructuradores del tipo: "provecho propio o ajeno" y "perjuicio de otro"; digamos que hay identidad estructural del tipo básico del artículo 194 y el tipo agravado del artículo 192-3 del C.P., con excepción al término de que el elemento ideológico del documento es de aquellos debe "permanecer en reserva".

El legislador español de 1995, al redactar los tipos agravados del tipo principal de "Descubrimiento y revelación de secretos" que afectaban a la intimidad presupuso en el artículo 197, varios de ellos atendiendo a su grado de insidiosidad, penetración, porosidad y afectación de la comunidad. Fue así como en el inciso 3º estructuró el tipo penal agravado por "revelación, difusión o cesión de datos, hechos o imágenes"; en el inciso 4º si las acciones las cometen los profesionales en el manejo y la responsabilidad de los administradores o encargados del uso o utilización de las bases de datos, registros o soportes informáticos, electrónicos o telemáticos; en el Inciso 5º, el acceso ilícito a los datos que componen "el núcleo duro de la privacy" o de acceso ilícito a la intimidad, que tiene como víctimas los mejores o incapaces; y en el inciso 6º , aquellos que tienen fines lucrativos y evita así hablar de "provecho" como un fin anfibológico.

Pues bien hubiese sido elogiable que el legislador del 2000, sistematizara de mejor forma posible el tipo delictivo 192 y sus correspondientes tipos penales agravados para evitar interpretaciones equivocas tan solo un elemento constitutivo como es el "de permanecer en reserva" un contenido de documento que es común al artículo 192-3 y 194 del C.P.

6.2.2.3.3. Ubicación. Titulo X, De los Delitos contra la Libertad Individual y otras Garantías, Capítulo VII: *Violación a la intimidad, reserva e interceptación de comunicaciones.*

Por lo dicho, anteriormente con una mejor redacción el presente delito autónomo podría haber sido un tipo agravado del tipo penal básico de violación ilícita de comunicaciones, ajustando

su punibilidad mayor cuando se trata de documentos “que deban permanecer en reserva” que es lo distintivo del ilícito del artículo 194 del C.P. Precisamente, la frase utilizada al final del ilícito demuestra la imperfección de construcción del delito, porque el legislador sospecha que algo falta para la perfección del tipo y por eso dice: “…siempre que la conducta no constituya delito sancionado con pena mayor”. Y es obvio, que si se trata de la punibilidad, el tipo penal agravado del artículo 192-3 tiene una pena de treinta y dos (32) a setenta y dos (72) meses; en cambio, el artículo 194 al presente tipo tan solo le impone una pena de multa sin cuantía prefijada.

6.2.2.3.4. Sujeto Activo: El agente del ilícito no tiene calificación alguna, por lo que puede cometerse por un particular o un servidor del Estado. Sin embargo, si se trata da servidor del estado, existen tres tipos penales básicos y sus correspondientes tipos penales agravados que le serían aplicados por su identidad, status de privilegio funcionarial y grado de responsabilidad y punibilidad mayores previstos en los artículos 418, 419 y 420 del C.P., bajo el bien jurídico tutelado en el Titulo XV, de los delitos contra la administración pública, Capítulo VIII, Del abuso de autoridad y otras infracciones.

En efecto, el primero se refiere (i) *Revelación de secreto.* El servidor público que indebidamente dé a conocer documento o noticia que deba mantener en secreto o reserva, incurrirá en multa y pérdida del empleo o cargo público (inciso 1º Artículo 418). Si de la conducta resultare perjuicio, la pena será de uno (1) a tres (3) años de prisión, multa de quince (15) a sesenta (60) salarios mínimos legales mensuales vigentes, e inhabilitación para el ejercicio de derechos y funciones públicas por cinco (5) años (Inciso 2º, ibíd.); (ii) *utilización de asunto sometido a secreto o reserva.* El servidor público que utilice en provecho propio o ajeno, descubrimiento científico, u otra información o dato llegados a su conocimiento por razón de sus funciones y que deban permanecer en secreto o reserva, incurrirá en multa y pérdida del empleo o cargo público, siempre que la conducta no constituya otro delito sancionado con pena mayor (Art. 419); (iii) *utilización indebida de información oficial privilegiada*. El servidor público que como empleado o directivo o miembro de una junta u órgano de administración de cualquier entidad pública, que haga uso indebido de información que haya conocido por razón o con ocasión de sus funciones y que no sea objeto de conocimiento público, con el fin de obtener provecho para sí o para un tercero, sea éste persona natural o jurídica, incurrirá en multa y pérdida del empleo o cargo público.

En nuestro país se debe complementar el delito de divulgación y empleo de documentos reservados prevista en el artículo 194 del C.P., para la generalidad de los casos de la prevista en los casos de delitos de divulgación de secretos especiales, cualquiera sea el soporte en el que se hallen éstos y bien sean cometidos por particulares como servidores públicos. En efecto, si los secretos son (i) de carácter político, económico o militar relacionados con la seguridad del Estado, el que indebidamente obtenga, emplee o revele dichos secretos incurrirá en prisión de 4 a 12 años de prisión, por el delito de espionaje (Art. 463); y (ii) Si los secretos obedecen a la invención científica, proceso o aplicación industrial o comercial, llegados a su conocimiento por razón de su cargo, oficio o profesión y estos son empleados, revelados o divulgados sabiendo que deben permanecer en reserva, incurrirá en prisión de 2 a 5 años y multa de 2000 SMMV, por el delito de *violación de reserva industrial o comercial* (artículo 308 del C.P.). Igual sanción obtendrá quien *indebidamente conozca, copie u obtenga secreto relacionado con descubrimiento, invención científica, proceso o aplicación industrial o comercial*. Las penas aumentan, si se *obtiene provecho propio o de tercero.*

Cuando se trata de un particular que realiza labores de apoderado o mandatario judicial (abogado litigante), cabría la aplicación del artículo 194 del C.P., porque al fin y al cabo, se está haciendo alusión en forma genérica a la divulgación o empleo del contenido de un documento que deba permanecer en reserva, sin adscribirlo a un tipo de personas

particulares por exclusión de otras que desempeñen o no una profesión. Entre el abogado litigante y su cliente, a partir de la suscripción del memorial poder y hasta aún después del cabal cumplimiento de las labores comprometidas con aquel, se realizan o conocen diversos documentos que ingresan a la categoría de permanecer en reserva para el mejor desempeño de las atribuciones conferidas en el poder como para salvaguardar derechos y libertades constitucionales como la intimidad, el honor o el buen nombre. En consecuencia, podría este tipo penal cubrir y proteger el derecho a *sigillum confessionis* entre abogados litigantes y clientes, si se dan todos los elementos de estructuración del tipo penal básico de divulgación o empleo de documentos reservados.

Ahora bien, la cláusula abierta que deja el tipo penal *in fine* del artículo 194 del C.P., presupone que si se dan los elementos estructurales del ilícito y éste resulta en la punibilidad de menor entidad, deberá aplicarse el tipo penal de mayor punición y más aún si dicha norma y tipo penal es de aplicación específica a los abogados litigantes.

En estas circunstancias estaríamos ante el tipo penal denominado de *infidelidad a los deberes profesionales* previsto en el artículo 445 del C.P., que tiene una pena de 1 a 4 años de prisión para el tipo penal básico y cometido en asuntos diferentes a la materia penal y de una pena aumentada hasta una tercera parte, si se realiza en asuntos de carácter penal. Esto por cuanto uno de los deberes profesionales del abogado es guardar la debida reserva de documentos, hechos, circunstancias o actos en sus relaciones profesionales con el cliente, pues estás pueden incidir en el éxito o fracaso del asunto encomendado a su cuidado, reserva y contratación de mandato (memorial poder). Si se ruptura, descubre, divulga o vulnera el derecho a *sigillum confessionis* se estructura una infidelidad de los deberes profesionales.

Dos de las diversas manifestaciones del *ius puniendi* del Estado [61], son (i) la investigación, juzgamiento y sanción de las conductas penales y contravencionales, a través de procesos, normas jurídicas aplicables a los tipos y las autoridades competentes. Al ámbito jurisdiccional penal, pertenecen las conductas delictivas comentadas de los artículos 194 y 445 del C.P.; y, (ii) En el ámbito sancionatorio disciplinario jurisdiccional, se investigan --tipos disciplinarios que guardan identidad con los tipos genéricos y especiales atribuidos a los abogados litigantes--, juzgan e imponen sanciones respectivas, por parte del Consejo Superior de la Judicatura, por disposición de la Ley 1123 de 2007 o Código Disciplinario del Abogado. En este ámbito, constituye falta disciplinaria contra la lealtad con el clienta: *Revelar o utilizar los secretos que le haya confiado el cliente, aun en virtud de reque-rimiento de autoridad, a menos que haya recibido autorización escrita de aquel, o que tenga necesidad de hacer revelaciones para evitar la comisión de un delito* (Art. 34-10).

En el derecho Penal Español, no existe este problema de interpretación y aplicabilidad de normas de mayor entidad punitiva o por remisión, pues se establece inequívocamente los delitos de violación al secreto profesional de quienes están obligados a éste según la Constitución y las leyes. En efecto, el artículo 199 del C.P del 95, se estructura como delito autónomo, las infracciones de los deberes de *sigilum profesionalis* y laborales, "*a quienes revelaren secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales".* Y como tipo penal agravado, "*cuando el profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona"*

De esta forma, el legislador ibérico atrae hacia el bien jurídico tutelado de la Intimidad, todas esas actuaciones de los profesionales (no solo los abogados, sino todos aquellos a ser "confidentes necesarios", como médicos, psicólogos, notarios, docentes, detectives privados,

---

(61) **RIASCOS GOMEZ, Libardo O.** ***El procedimiento disciplinario de los abogados litigantes en la Ley 1123 de 2007.*** *Editorial Ibañez, Bogotá, 2010, pág. 98 y ss.*

profesionales del sector financiero o bancario, profesionales del sector informático, etc.) que faltaban a sus deberes en la profesión con relación al cliente y que constituían "delitos formales o de mera desobediencia". Así las actuaciones de los profesionales dirigidas a violar el secreto profesional vulneran el bien jurídico de la intimidad "*y no intereses corporativos-gremiales, centrados en la idea de rectitud del ejercicio profesional, pues esa dimensión es la contemplada prioritariamente en las normas sectoriales de deontología profesional"* **[62].**

6.2.2.3.5. Conceptualizaciones. Tres conceptualizaciones en el presente tipo parecen tener algo de discusión: (i) El documento; (ii) Permanecer en reserva; y (iii) Documento Público.

Sobre el primero, el artículo 294 del C.P., suministra una definición parecida a la vertida por el artículo 255 del C.P., del 80, así: es documento toda expresión de persona conocida o conocible recogida por escrito o por cualquier medio mecánico o técnicamente impreso, *soporte material que exprese o incorpore datos o hechos*, que tengan capacidad probatoria.

Aquí caben las observaciones realizadas a la utilización del término documento, más restrictivo que el término "escrito", como inicialmente se planteo por los reformadores del C.P., del 80 y que no abarcaba los que técnica y jurídicamente no eran considerados documentos, como podrían ser las cartas, tarjetas postales, telegramas, papeles con mensajes de texto, etc. Igualmente que la definición de documento por la ubicación en el C.P., sólo es aplicable a los delitos de falsedad documental y no a los que están por fuera de ese título IX, de los Delitos contra la fe pública y Capítulo III, de los delitos de falsedad en documentos. Para que sea aplicable a todo el Código debería estar en la parte general de dicho Código.

Es oportuno comparar el término documento utilizado por el artículo 255, el cual sostiene: "*Para efecto de los artículos anteriores se asimilan a documentos, siempre que puedan servir de prueba, las expresiones de persona conocida o conocible recogidas por cualquier medio mecánico, los planos, dibujos, cuadros, fotografías, cintas cinematográficas, radiográficas, fono-ópticas, archivos electromagnéticos y registro técnico impreso*".

Esta definición toma al documento más desde un punto de vista casuístico que jurídico, pero es útil a los eventos de tomar los ejemplos dados como elementos asimilables a documentos según la evolución de las tecnologías que captan imágenes, sonidos y audio o voz y según las nuevas tecnologías de la información y la comunicación o TIC. Además la definición sirve para indicar algo que es esencial en la definición jurídica de documento, cual es, la determinación que esos ejemplos "*deban servir de prueba"* y sean "*expresiones de persona conocida y conocible*". En efecto, estos elementos son de capital importancia a la hora de determinar si se reputa o no documento y sirve a los fines judiciales respectivos.

La nueva definición de documento en el C.P., del 2000, coincide en estos dos últimos elementos de la definición jurídica de documento. Obvia los ejemplos de documentos y se centra en la forma de verificación de los documentos (escrito, mecánico o tecnológico), como en el soporte en el que se expresa o incorpora datos o hechos. Esta definición es más jurídica y de ella fácilmente se puede deducir que el documento puede ser escrito, mecánico o por vía de las nuevas tecnologías de la informática (mensajes de datos en pantalla, sin desplazamiento físico a soportes de papel o impresos), electrónica (p.e. fax) y telemática (mensajes de datos en la Internet u *On line*).

---

(62) MORALES PRATS, *Fermín.* ***Delitos contra…*** *Ob., ut supra cit., p. 325*

El Código Penal Español contiene la definición de documento en la parte general del Código, a efectos de la aplicabilidad en toda la parte especial y huye de las concepciones tradicionales de identificar al documento con la escritura y el papel, "*para adecuarse al cualquier tipo de soporte capaz de contener datos con relevancia jurídica, como los soportes informáticos"* (artículo 26)

El STS (Sala 2ª) de 19 de abril de 1991, anotaba que "*el concepto de documento actualmente no puede reservarse y ceñirse con exclusividad al papel reflejo y receptor por escrito de una declaración humana, desde el momento que nuevas técnicas han multiplicado las ofertas de soportes físicos capaces de corporeizar y dotar de perpetuación al pensamiento y a la declaración de voluntad; una grabación de video, o cinematográfica, un disco o una cinta magnetofónica, los disquetes informáticos, portadores de manifestaciones y acreditamientos, con vocación probatoria, pueden ser susceptibles de manipulación falsaria al igual que un documento escrito…*" **[63]**

Permanecer en reserva, significa que el contenido del documento sólo debe ser conocido por quienes estén autorizados para hacerlo por disposición de las normas jurídicas o por el cumplimiento de las labores del cargo, profesión u oficio, y una vez éste conocimiento se aprehenda por los medios tradicionales o tecnológicos TIC, deberá guardar o custodiar el contenido del mismo.

Todos tienen derecho de acceso al documento público, salvo los casos previstos en la ley, según el artículo 74, constitucional. Este precepto constitucional estaba reglamentado preconstitucionalmente desde la Ley 57 de 1985 o estatuto de la Información pública.

Esto significa que el tipo penal previsto en el artículo 194 del C.P., de 2000, no es aplicable a los documentos públicos, ni a su parte ideológica, por cuanto la regla general en los documentos privados es la reserva y por excepción, su revelación, divulgación o cesión, previa autorización legal o judicial; en cambio, en el documento público, la regla y la excepción son a la inversa.

En efecto, la Ley 57 de 1985 o Estatuto de la Información y la publicidad de los Documentos Públicos, estipula unos principios sobre la reserva de los documentos públicos, así: (i) Si un documento es reservado el secreto se aplicará exclusivamente a dicho documento y no a las demás piezas del respectivo expediente o negocio administrativo o disciplinario (parágrafo del artículo 19); (ii) El carácter reservado de un documento no será oponible a las autoridades que lo soliciten para el debido ejercicio de sus funciones./ Corresponde a dichas autoridades asegurar la reserva de los documentos que lleguen a conocer en desarrollo de lo prescrito en este artículo (Incisos 1º y 2º del artículo 20); (iii) La Administración sólo podrá negar la consulta de determinados documentos o la copia o fotocopia de los mismos mediante providencia motivada que señale su carácter reservado, indicando las disposiciones legales pertinentes (artículo 21); (iv) El Departamento Administrativo Nacional de Estadística (DANE), por conducto del Banco Nacional de Datos, organizará un servicio informativo que suministre al público copia de los documentos a que se refiere la presente Ley (artículo 26); (v) Son oficinas públicas las de las corporaciones de elección popular./ En consecuencia, los documentos que en ellas reposen son consultables por los particulares y de los mismos se pueden pedir copias o fotocopias, únicamente con las limitaciones impuestas por el carácter reservado que algunos de ellos tengan (artículo 27).

---

(63) Citada por SANCHIS CRESPO, Carolina**. *La fe documental y la prueba tecnológica.*** En: AA.VV. El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales. Estudios de Derecho Penal y criminología, Editorial Comares S.L., Granada, 2006, p. 208 y ss.

Ley 190 de 1995 o Estatuto anticorrupción, también estipula unos principios sobre la reserva documental pública: (i) *Harán parte de la reserva las investigaciones preliminares, los pliegos y autos de cargos que formulen la Procuraduría General de la Nación y demás órganos de control dentro de los procesos disciplinarios y de responsabilidad fiscal, lo mismo que los respectivos descargos; los fallos serán públicos* (artículo 33-1); (ii) La violación de la reserva será causal de mala conducta (Parágrafo 1º del artículo 33); (iii) En el evento de que se conozca la información reservada, la entidad deberá verificar una investigación interna y explicarle a la opinión las posibles razones del hecho (Parágrafo 1º del artículo 33); (iv) En las investigaciones penales la reserva de la instrucción no impedirá a los funcionarios competentes proporcionar a los medios de comunicación información sobre algunos aspectos (artículo 78); (v) La decisión de negar el acceso a los documentos públicos será siempre motivada, con base en la existencia de reserva legal o constitucional, o cuando exista norma especial que atribuya facultad de informar a un funcionario de superior jerarquía (Inciso 2º del artículo 79).

La Ley 594 de 2000, La ley General de Archivos, establece una serie de principios sobre la reserva documental presente en los archivos públicos y privados, así: (i) prevé en el artículo 27 que *"Todas las personas tienen derecho a consultar los documentos de archivos públicos y a que se les expida copia de los mismos, siempre que dichos documentos no tengan carácter reservado conforme a la Constitución o a la ley".* Y agrega el inciso 2º*, "Las autoridades responsables de los archivos públicos y privados garantizarán el derecho a la intimidad personal y familiar, honra y buen nombre de las personas y demás derechos consagrados en la Constitución y las leyes";* (ii) La reserva legal sobre cualquier documento cesará a los treinta años de su expedición. Cumplidos éstos, el documento por este solo hecho no adquiere el carácter histórico y podrá ser consultado por cualquier ciudadano, y la autoridad que esté en su posesión adquiere la obligación de expedir a quien lo demande copias o fotocopias del mismo" (artículo 28).

6.2.2.3.6. Verbos alternativos: divulgar o emplear. La configuración del tipo penal básico se realiza con acciones alternativas sobre el elemento ideológico del documento que debe permanecer en reserva, generalmente de documentos privados, pues los públicos como se ha dicho la reserva es una excepción.

En este aparte también son válidas las observaciones realizadas al estudiar idéntico tipo penal en el Código Penal de 1980, con las diferencias de punibilidad que para ese entonces resultan mayores y de más trascendencia jurídica que las asignadas al actual tipo penal del artículo 194 del C.P.

6.2.2.3.7. Tipo penal agravado de descubrimiento de información reservada contenida en un documento.

El Código Penal Español del 95, en el artículo 197-3, instituyó como tipo penal agravado la revelación, difusión o cesión de datos, hechos o imágenes y aplicable a los tipos penales básicos de apoderamiento de documentos o efectos personales, al de control audio-visual clandestino y al relativo a los abusos informáticos.

Este tipo agravado tiene, entre otras las siguientes particularidades: (i) Presenta con relación a los demás tipos básicos un incremento de menoscabo a la intimidad; (ii) Este delito se comporta como un tipo penal compuesto (estructura típica doble [64]) que requiere la previa comisión de uno de los tipos penales básico, por eso no opera como un tipo penal de indiscre-

---

(64) MORALES PRATS, *Fermín**. Delitos contra…** Ob., ut supra cit., p. 325*

ción autónomo; (iii) Este tipo penal agravado a diferencia del tipo penal de divulgación o empleo de documentos reservados, no sólo se extiende a la "revelación" o divulgación propiamente dicha, sino que va más allá con la cesión o transferencia de datos personales "*automatizados a paraísos informáticos, esto es, a países que no ofrecen el mínimo esencial de garantía estándar, sobre el habeas data o libertad informática de los ciudadanos…*" **[65].**

6.2.2.3.7.1. Aumento de Penas: El tipo penal de divulgación y empleo de documentos reservados en su versión original tenía una punibilidad de multa que no se compadecía ni con el bien jurídico protegido de la intimidad, reserva y comunicaciones, ni con el despliegue de acciones comisivas del tipo reforzadas con dos elementos estructuradores del tipo de aprovechamiento genérico (provecho propio o ajeno o con perjuicio de otro. Es decir el provecho no sólo es económico, sino personal, político, sicológico, sexual, étnico, etc.). Sin embargo, Este tipo penal aumento su punibilidad basado en el criterio de protección y garantía de la reserva legal de documentos de inteligencia y contrainteligencia mediante la Ley 1288 de 2009, relativa a las "*normas para fortalecer el marco legal que permite a los organismos, que llevan a cabo actividades de inteligencia y contrainteligencia…*". En efecto, se aumentan la pena de prisión de cinco (5) a ocho (8) años.

6.2.2.4. Delito de Violación Ilícita de comunicaciones o correspondencia de carácter oficial

6.2.2.4.1. Fuente normativa: Artículo 196 C.P., reformado parcialmente por la (i) Ley 890 de 2004, artículo 14, en cuanto aumento de penas, a partir del 1º de Enero de 2005; (ii) La Ley 1341 de 2009, sobre la conceptualización de los nuevos medios de la información y la comunicación o TIC, régimen jurídico de la telefonía fija y móvil e infracciones contravencionales que afectan al derecho de la intimidad, el honor y demás libertades y derechos constitucionales cuando existen actuaciones ilícitas en las comunicaciones.

Son aplicables al tipo las siguientes normas especiales y procesales:

(i) La Ley 527 de 1992, referido a la conceptualización de los sistemas de información y datos y los mensajes de datos p.e. mensaje de correo electrónico o el Intercambio electrónico de documentos EDI;

(iv) El Decreto 075 de 2006 de Enero 13, sobre las obligaciones que le asisten a los operadores de servicios de telecomunicaciones en procura de optimizar la labor de investigación de los delitos por parte de las autoridades competentes (Fiscalía General de la Nación) y artículo 235 del C.P.P. (Ley 906 de 2004), reformado por la Ley 1142 de 2007, sobre la interceptación de comunicaciones telefónicas y similares ordenadas por la Fiscalía, "con el objeto de buscar elementos materiales probatorios, evidencia física, búsqueda y ubicación de imputados o indiciados que se intercepten mediante grabación magnetofónica o similares de comunicaciones telefónicas, radiotelefónicas y similares que utilicen el espacio electromagnético, cuya información tengan interés para los fines de la actuación"; y,

(v) El artículo 447 del C.P., reformado por el artículo 45 de la Ley 1142 de 2007, atinente al derecho de receptación sobre bienes o inmuebles destinados a las comunicaciones telefónicas, telegráficas, informáticas, telemáticas y satelitales.

---

(65) MORALES PRATS, *Fermín**. Delitos contra…** Ob., ut supra cit., p. 325*

6.2.2.4.2. Tipo penal. *El que ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida comunicación o correspondencia de carácter oficial, incurrirá en prisión de cuarenta y ocho (48) a ciento ocho (108) meses.*

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.

6.2.2.4.3. Ubicación: Título III, *de los Delitos contra la Libertad Individual y otras garantías*, Capítulo VII, *Violación a la intimidad, reserva e interceptación de comunicaciones*.

6.2.2.4.4. Sujetos activos: Al igual que los anteriores tipos penales en el presente no se requiere calificación especial alguna para ser agente comisivo del delito.

6.2.2.4.5. Conceptualizaciones. Los conceptos vertidos en los tipos básicos y agravados anteriores son válidos en el presente tipo penal, especialmente sobre comunicaciones verbales, escritas o por correspondencia (cartas, tarjetas postales, papeles con mensajes, etc.) y nuevas tecnologías de la información y las comunicaciones o TIC –por medios informáticos, electrónicos y telemáticos--. Así como también sobre los mensajes de datos y entre ellos: los mensajes de Correo electrónico o "e-mail", los documentos de intercambio electrónico o EDI; al igual que sobre las comunicaciones tradicionales telefónicas, telegráficas (v.gr. telegrama); el fax como comunicación electrónica.

Ahora bien, lo que el tipo penal reprime es la interceptación de comunicaciones de carácter oficial realizada ilegalmente por personas particulares o servidores del Estado. Sin embargo, las interceptaciones legales y conforme a derecho están reguladas en el Decreto 075 de Enero 13 de 2006.

En este estatuto del Ministerio de Comunicaciones se establece las directrices para la realización de las interceptaciones legales en Colombia por parte de la Fiscalía General de la Nación en busca de elementos materiales probatorios, evidencia física y ubicación de imputados o indiciados; así como también, cuáles son tecnologías aplicables para la interceptación (Software y hardware, incluidas las licencias para el desarrollo de esa labor); los recursos técnicos utilizados en las telecomunicaciones; las obligaciones de los operadores de servicios de telecomunicaciones de telefonía móvil celular, PCS y de sistemas de Acceso troncalizado que operan en el territorio nacional, los cuales deben garantizar la interceptación remota de las comunicaciones para que la Fiscalía o las entidades que autorice la ley cumplan su misión y objetivos.

Por lo anterior, el objetivo principal y único de la Interceptación (Intercepción) combatir las actividades delictuales.

Interceptación y Grabación. "La vigilancia e interceptación de las telecomunicaciones toca unas zonas muy sensibles de la ciudadanía que no se encuentra conforme con que se invada un derecho fundamental, que en muchos países está protegido constitucionalmente, alegando que dichas actuaciones responden a necesidades de la seguridad nacional. Por tanto, para poder invadir el derecho a la intimidad cualquier procedimiento de interceptación debe comenzar teniendo un fundamento legal y unos motivos éticos muy claros y sólidos.

En las redes telefónicas antiguas era relativamente sencillo efectuar escuchas, tanto legales por orden judicial, como ilegales. Como se establecía y dedicaba un circuito de voz para cada conversación y los terminales eran muy sencillos, resultaba fácil interceptar la comunicación en algún punto o poner la llamada en conferencia con el lugar de intercepción, donde quedaba

grabada la conversación. Sin embargo, los tiempos han cambiado;… (la) intercepción de conversaciones de voz y de datos en nuestros días… son más complejos [66].

…la obligación legal de grabar las llamadas a los centros de emergencia, las transacciones bancarias por vía telefónica, la compraventa de valores y otras obligaciones similares de grabación no se consideran intercepción, sino una grabación en destino que se supone conocida por el llamante, a quien se le advierte de algún modo, y que generalmente se efectúa por la entidad que recibe la llamada" [67].

En nuestro país la interceptación legal, a partir de la Constitución de 1991, artículo 250-2, se adscribió a la Fiscalía General de la Nación y el juez competente que ejerce "*las funciones de control de garantías efectuará el control posterior respectivo, a más tardar dentro de las treinta y seis (36) horas siguientes,* ***al solo efecto de determinar su validez***". Este último aparte fue declarado inexequible mediante de la Corte Constitucional Sentencia C-1092-2003 [68].

El artículo 351 del referido Decreto 2700 de 1991, sobre *interceptación de comunicaciones*, estableció las siguientes pautas de obligada observancia en aquella época: (i) En la etapa de investigación penal, podrá ser ordenada por orden motivada y por escrito, por la Dirección Nacional de Fiscalías. En el juzgamiento lo será el juez competente; (ii) El único objetivo es buscar pruebas judiciales; (iii) Las comunicaciones telefónicas, radiotelefónicas y similares, se interceptan mediante grabación magnetofónica y dicha grabación se agregará al expediente para los fines del proceso. Tales grabaciones se trasladarán al expediente, por medio de escrito certificado por el respectivo funcionario; (iv) De lo anterior se deduce, que no se pueden escuchar directamente las conversaciones telefónicas sino grabarlas con fines

---

(66) "**Telefonía fija.** Las redes del servicio telefónico disponible al público (STDP) moderno disponen en sus centrales de técnicas y servicios para realizar intercepciones legales automáticas. Los sistemas de gestión de intercepciones sirven para grabar voz y/o datos de abonados… De lo anterior se desprende que con la colaboración del operador correspondiente resulta sencillo ordenar y efectuar escuchas legales en el servicio telefónico fijo disponible al público (STDP).
Telefonía Móvil. La intercepción de la telefonía móvil digital, por tanto con conmutación de paquetes, es una de las cuestiones más candentes, en particular a raíz del escándalo de las escuchas en la telefonía móvil de Atenas, (*Realizadas al Primer Ministro y otras personalidades en la red GSM de Vodafone…*) que "puso el dedo en la llaga" o cuestión de fondo, si con métodos automáticos de interceptación no se estará creando un mayor riesgo de seguridad: si son automáticas y las maneja personal del operador quizás se esté abriendo una vía para que personas menos honorables manipulen el sistema en su propio beneficio. Un estudio de ITAA, citado más arriba en la sección de telefonía fija, entendió que el problema de las escuchas en Atenas fue obra de personal interno a la compañía y no de alguien ajeno a ella. Lo mismo parece que ha ocurrido recientemente en Colombia ("En Fiscalía se usaron órdenes legales para escuchar ilegalmente a" varias personalidades… EL TIEMPO…") En todo caso, queda evidenciado lo sencillo que resulta interceptar las comunicaciones móviles digitales bajo mandato legal, y como también se puede hacer ilegalmente.
Telefonía IP… cuando se emplean técnicas de Telefonía IP de "Filosofía Internet", la cuestión es bastante más compleja. En el contexto que nos ocupa, de intercepción legal de conversaciones y datos, cuando la conversación a interceptar se establece mediante telefonía IP, con protocolos de señalización normalizados como SIP que están absolutamente separados del flujo de datos, hay que diferenciar: quién conoce que el sujeto tiene interceptadas las llamadas, quién conoce el inicio de las sesiones y quién proporciona el acceso a la red…"
VoIP. La interceptación de llamadas en servicios vocales que no tienen interconexión con el STDP no es muy diferente del caso de la Telefonía IP. Será el operador de acceso quien se ocupe de recoger las comunicaciones interceptadas, si bien los jueces podrán exigir al operador del servicio que proporcione los metadatos que disponga.
Interceptación de datos en el transporte o Backbone. También hay equipos de interceptación que pueden trabajar en las redes de transporte, incluso sobre flujos de gigabit, extrayendo los paquetes de interés". **En:** http://es.wikitel.info/wiki/Interceptaci%C3%B3n_Legal

(67) **En:** http://es.wikitel.info/wiki/Interceptaci%C3%B3n_Legal

(68) "Para la Corte es claro que la expresión ´validez´…, es de un valor jurídico incierto en el texto constitucional…" En: AA.VV. ***Constitución Política de Colombia***. Editorial Legis S.A., Bogotá, p. 3052

judiciales; (v) Las personas que participen en estas diligencias se obligan a guardar la debida reserva; (vi) Por ningún motivo se podrán interceptar las comunicaciones del defensor; y v) El funcionario dispondrá la práctica de las pruebas necesarias para identificar a las personas entre quienes se hubiere realizado la comunicación telefónica llevada al proceso en grabación.

"En caso de flagrancia las autoridades de policía judicial podrán interceptar y reproducir las comunicaciones con el objeto de buscar pruebas", según rezaba el inciso in fine del artículo 351. Este texto fue declarado inconstitucional, mediante Sentencia C-657-1996 puesto que, "*en ningún evento podrá procederse a interceptar o a registrar la correspondencia y las demás formas de comunicación privada sin que medie la orden judicial. Lo que corresponde al dominio legal es el señalamiento [de] los casos y del procedimiento, más no está autorizada la ley para dispensar de la orden judicial*" **[69]**

La Ley 600 de 2000, Julio 24, en parecidos términos, el artículo 301 del C.P.P., expuso las directrices de la interceptación legal de las comunicaciones, con pequeñas diferencias: (i) Se adicionó a las comunicaciones "similares" la expresión "que utilicen el espectro electromagnético; (ii) Dispone que "las entidades encargadas de la operación técnica de la respectiva interceptación, tienen la obligación de realizar la misma dentro de las cuarenta y ocho (48) horas siguientes a la notificación de la orden"; (iii) Cuando se trate de interceptación durante la etapa de la investigación la decisión debe ser remitida dentro de las veinticuatro (24) horas siguientes a la Dirección Nacional de Fiscalías; y, (iv) Según el artículo 293 del C.P.P., "Providencias Reservadas. Las providencias motivadas mediante las cuales se disponga el allanamiento y el registro, la retención de correspondencia postal o telegráfica o la interceptación de comunicaciones telefónicas, no se darán a conocer a las partes mientras el funcionario considere que ello puede interferir en el desarrollo de la respectiva diligencia. Contra dichas providencias no procede recurso alguno".

El artículo 235 del actual C.P.P., (Ley 906 de 2004, reformada por la Ley 1142 de 2007) retomó en gran parte las pautas y directrices sobre la interceptación legal de los anteriores Códigos de procedimiento penal y cambió los términos de cumplimiento de la orden judicial impartida por la Fiscalía para realizar la operación técnica de la interceptación en forma "inmediata". Estableció un término de vigencia máxima de la orden de interceptación que no traían las anteriores normas procesales penales y lo dejó en tres (3) meses y prorrogable hasta otro tanto, "***a juicio del fiscal",*** si "subsisten los motivos fundados que la originaron". Esta actuación es examinada por el Juez.

La Corte Constitucional en sentencia C-131-2009, decidió que el término "*a juicio del fiscal*" del artículo 235 del C.P.P, fue declarado constitucional "*bajo el entendido de que en todo caso, la orden del Fiscal de prorrogar la interceptación de comunicaciones y similares deberá ser sometida al control previo de legalidad por parte del Juez de Control de Garantías*". Esto por cuanto en anteriores pronunciamientos, la Corte se había expresado que "la afectación (limitación o restricción) de derechos fundamentales (vgr. La intimidad) *"obliga al Fiscal a solicitar de manera expresa y específica la autorización judicial previa"* (C-822-2005).

Finalmente rige hasta nuestros días las pautas jurisprudenciales dadas por la Corte Constitucional, sobre interceptaciones a las comunicaciones. En efecto, la Corte "*en guarda de la cabal interpretación y aplicación de las normas constitucionales enunciadas y de los*

---

(69) Citado por la ***Academia Colombiana de Jurisprudencia*** al absolver una consulta sobre la vigencia de normas relativas a la interceptación legal de las comunicaciones entre 1998 y 1999. Concepto de 13 de Abril de 2009. En: http://www.acj.org.co/conceptos/concep_ord_009-2009.htm

tratados internacionales sobre derechos humanos, que han sido estrictos y celosos en la materia (Cfr. Convención Americana sobre Derechos Humanos, "Pacto de San José de Costa Rica", aprobada mediante Ley 16 de 1992, artículo 11; Pacto Internacional de Derechos Civiles y Políticos, aprobado por Ley 78 de 1968, artículo 17), debe declarar sin ambages que ninguna persona pública ni privada, por plausible o encomiable que sea el objetivo perseguido, está autorizada para interceptar, escuchar, grabar, difundir ni transcribir las comunicaciones privadas, esto es, las que tienen lugar entre las personas mediante conversación directa, o por la transmisión o registro de mensajes, merced a la utilización de medios técnicos o electrónicos aptos para ello, tales como teléfonos convencionales o celulares, radioteléfonos, citófonos, buscapersonas, equipos de radiocomunicaciones, entre otros, A MENOS QUE EXISTA PREVIA Y ESPECIFICA ORDEN JUDICIAL Y QUE ELLA SE HAYA IMPARTIDO EN EL CURSO DE PROCESOS, EN LOS CASOS Y CON LAS FORMALIDADES QUE ESTABLEZCA LA LEY, según los perentorios términos del artículo 15 de la Constitución Política" (Sentencia C-626-1996 y reiterada en la Sentencia C-131-2009).

6.2.2.4.6. Verbos alternativos: sustraer, ocultar, extraviar, destruir, interceptar, controlar e impedir. En cuanto a la estructuración del tipo penal básico, son válidos las observaciones y comentarios realizados en el tipo penal de violación ilícita de la correspondencia y comunicaciones privadas (artículo 192 del C.P.).

6.2.2.4.7. Tipo básico autónomo de interceptación o violación de correspondencia y comunicaciones "oficiales".

El tipo básico y autónomo de interceptación o violación de correspondencia y comunicaciones oficiales, fue creado por el legislador penal del 2000, pues en el C.P., de 1980 permanecía fusionado junto a violación de correspondencia y comunicaciones de carácter privado en el artículo 288, con una punibilidad menor tanto en el tipo básico como en el agravado. Es cierto que se gana en la redacción y la separabilidad de los tipos penales cuando se vulnera intereses y derechos de carácter particular o bien de carácter público, pero también es cierto que en cuanto a la insidiosidad de los mismos se sigue produciendo un incremento de menoscabo a los derechos fundamentales como la intimidad personal y familiar con acciones dirigidas a violar la correspondencia y las comunicaciones, sean éstas de carácter privado o público. Es coherente también en cuanto a la mayor punibilidad cuando las acciones o conductas punitivas se comenten contra las comunicaciones (cualquiera sea la forma y medios utilizados) de carácter público.

6.2.2.4.8. Tipo agravado por interceptación o violación de correspondencia y comunicaciones de carácter oficial que pertenece a algunos organismos del Estado.

El inciso 2º del artículo 196 del C.P., establece el tipo penal agravado cuando la violación ilícita de las comunicaciones o correspondencia oficial perteneciente a la rama judicial o a los organismos de control o seguridad del Estado. Se entiende que aquí hay una estructura típica doble (Tipo penal compuesto), pues tiene que darse la violación ilícita de las comunicaciones, para que se presente la agravación del tipo cuando la correspondencia o las comunicaciones le pertenecen a las los jueces individuales o colegiados de todas las ramas o áreas del derecho (Constitucional, Administrativo, Penal, Civil, Laboral, de Familia, etc.,), a los fiscales de todos los ámbitos y materias de protección e investigación penal en Colombia, como los Fiscales delegados ante Juzgados, Tribunales y Cortes, así como el Vicefiscal y Fiscal General de la Fiscalía General de la República; entre otros, pertenecientes a la Rama Judicial de Colombia. Así mismo, a los Contralores municipales, departamentales, distritales y General de la República (como órganos de control fiscal); a los Personeros Municipales, Procuradores Provinciales, Regionales y General de la República (como órganos de control de la conducta

de los servidores del Estado) y a los defensores seccionales y al nacional de Colombia (perteneciente a la Procuraduría General de la Nación). Finalmente, cuando se vulnera la correspondencia o comunicaciones dirigida a los miembros de la Fuerzas Pública Colombiana (Fuerzas militares y la Policía Nacional. Artículos 216 y ss., constitucionales) y los demás organismos de seguridad como el DAS.

6.2.2.4.9. Aumento de Penas: Para el tipo penal básico como agravado de interceptación o violación de correspondencia o de comunicaciones oficiales, la punibilidad aumento de uno a cuatro años y de tres a nueve años de Prisión, en relación con las penas originales del C.P., del 2000. Así mismo, aumentará hasta en una tercera parte cuando la comunicación y correspondencia esté destinada a la rama judicial o a los organismos de control o de seguridad del Estado, según la Ley 890 de 2004, artículo 14.

7. LA INTIMIDAD EN EL CODIGO PENAL ESPAÑOL DE 1995

En el presente aparte, haremos un breve comentario a los tipos penales básicos y agravados que atentan a la "Intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", previstos en el Titulo X del Código Penal de 1995.

7.1. Ubicación normativa de los tipos penales

A. Capítulo Primero: Descubrimiento y revelación de Secretos: En el artículo 197, se presentan tres tipos penales básicos y cuatro tipos penales agravados. En el artículo 198, un tipo básico de indiscreción. En el artículo 199-1, un tipo de indiscreción en las relaciones laborales. En el Artículo 199-2, un tipo básico de vulneración del deber de secreto profesional. En el artículo 200, un tipo básico contra intimidad de los datos reservados de las personas jurídicas.

2. Capítulo Segundo: Allanamiento de morada, domicilio de personas jurídicas y establecimientos abiertos al público. En el artículo 2002**,** la modalidad típica tradicional de allanamiento de morada, relativa a las figuras típicas básicas de entrada en morada ajena y de mantenimiento en la misma contra la voluntad del morador, y el tipo agravado consistente en la perpetración de las conductas típicas básicas con violencia o intimidación (Artículo 202). Allanamiento de morada en la extensión de la figura delictiva al domicilio de las personas jurídicas y los establecimientos abiertos al público (artículo 203) y las violaciones domiciliarias de funcionarios, llevadas a cabo mediando una causa penal, pero sin relación con la misma (artículo 204).

7.2. Breve análisis del Artículo 197 del C.P.

1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3. Se impondrá pena de prisión de dos a cinco años, si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y si haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

4. Si los hechos descritos en los apartes 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.

6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 y 2 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en apartado 5, la pena a imponer será de prisión de cuatro a siete años.

En el artículo 197-1, encontramos los siguientes tipos penales básicos:

1. Apoderamiento de documentos (papeles, cartas, mensajes de correo electrónico, etc.) **y efectos personales.**

2. Control visual y clandestino, por medio de la interceptación de telecomunicaciones o de la utilización de los artificios técnicos de escucha, transmisión, grabación o reproducción de sonido o de la imagen, o con “cualquier otro tipo de comunicación” (v.gr. Telefax o Internet).

En el art.197-2, el tipo penal autónomo de **“Abusos informáticos”,** sobre datos personales automatizados o no (ficheros o bases de datos manuales).

Cuatro tipos penales agravados, así:

1. Por difusión, revelación o cesión a terceros de los datos, hechos o imágenes. (Art.197-3)
2. Por la condición del sujeto activo –en-cargados o responsables de ficheros o bancos automatizados, archivos o registros– (Art.197-4)

3. Por afectación del núcleo duro de la “Privacy” o bien en el hecho de que la conducta atentatoria a la intimidad tenga como víctima a un menor de edad (Art.197-5)

4. Por realizar las conductas con fines lucrativos (Art. 197-6)

Delito de Indiscreción, relativo a la conducta del sujeto que, con conocimiento de su origen ilícito y sin haber tomado parte de su descubrimiento (por consiguiente sin necesidad de haber realizado alguna de las conductas de los tipos 1º y 2º , difunde, revela o cede a terceros datos, hechos o imágenes (Art.198 CP).

Delito de indiscreción en las relaciones laborales, basado en la toma de conocimiento o acceso ilícito a la intimidad por razón del oficio o de la relación laboral, consistente en la revelación de la misma a terceros ilícita (Art. 199-1)

Delito de vulneración del deber profesional. Conocimiento y acceso ilícito de la intimidad del cliente o de terceros por el profesional: Datos, hechos, acciones quedan en la esfera de la confidencialidad, la conducta queda fijada en un acto ilícito de revelación a terceros (Art.199-2). Violación del "*Sigilium confessionis*": médicos, abogados, detectives privados, banqueros, del sector informático (Art. 199-2).

Delito contra la intimidad de los datos reservados de las personas jurídicas (Art. 200).

III. DELITOS CONTRA LOS DATOS PERSONALES Y EL HABEAS DATA [1]

1. COMO SURGE EL TÉRMINO "HABEAS DATA"

El términos "*Habeas Data*" que hoy universalmente conoce el ámbito del derecho como una eficaz y expedita institución jurídica constitucional y legislativa para la defensa y protección de los datos o informaciones personales y el pleno ejercicio de los derechos y las libertades constitucionales, ha tenido una explicación etimológica generalizada y homologada en los Estados latinoamericanos y principalmente en Brasil donde nace la institución con dicho nombre.

El constitucionalismo brasileño en 1988, creó el "remedio" o acción procedimental del Hábeas Data como un mecanismo jurídico-constitucional preventivo para el acceso y el conocimiento de los datos o informaciones personales y como un instrumento sancionatorio, de corrección, actualización y supresión de datos cuanto estos son incorrectos. En el desarrollo legislativo nueve años después, el Hábeas Data se convirtió en una acción exhibitoria de los datos personales de carácter civil y administrativo, según la naturaleza jurídica de las personas naturales o jurídicas que manejen los datos. El legislador volvió sus ojos al origen de la institución jurídica románica: un interdicto exhibitorio de acta o de documento.

El Término Habeas Data, se dice proviene del término inglés de "Data" o datos, o del singular "Datum" dato, es el que se le aplica por agregación a la definición del "Hábeas" latino, pues como lo demuestra *Puccenilli* [2], el término data no significa datos ni su singular dato en latín, como casi todos los lectores por vez primera de los términos "Hábeas Data" deducen fonológicamente. Al principio de esta Obra también hicimos alusión a ese desfase lexical que va más allá del simple uso de términos latinos e ingleses unidos para explicar una institución jurídica que se convierte en un mecanismo constitucional y legal de protección y defensa de otros derechos de igual rango.

2. LA CONCEPTUALIZACION DEL HABEAS DATA

2.1. El Hábeas Data en la Constitución Colombia es una acción de tutela específica de tipo jurisdiccional o una vía administrativa

El Hábeas Data en la Constitución Colombia es una acción de tutela específica de tipo jurisdiccional o vía administrativa que protege todas las fases del tratamiento de los datos personales y los derechos constitucionales, entre ellos el de la intimidad y el buen nombre.

La Institución jurídica colombiana del Hábeas Data se estructura a partir del inciso 1º y 2º del artículo 15, el artículo 20 y 74 de la Constitución de 1991. A saber: "*Todas las personas tiene derecho a su intimidad personal y familiar y a su buen nombre… De igual modo, tienen 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".* Agrega el inciso segundo, "*En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución*".

El artículo 20, a su turno reza: "*Se garantiza a toda persona la libertad… (de) informar y recibir información veraz e imparcial…*"

---

(1) RIASCOS GOMEZ, Libardo O. ***El habeas data: visión constitucional, legal y punitiva.*** Editorial Universidad de Nariño, ISBN. 978-958-8609-08-9. Pasto, 2011, p. 587 y ss.

(2) PUCCINELLI, Oscar. ***El Hábeas Data en el Brasil.*** En: www.astrea.com

Por su parte el artículo 74, sostiene: "*Todas las personas tienen derecho a acceder a los documentos públicos…*"

En la primera norma se encuentra el núcleo esencial del Hábeas Data, pues mientras en el inciso 1º se confiere el ejercicio de la acción de tutela específica a toda persona natural o jurídica para que pueda aprehender el conocimiento de las informaciones o datos personales que le conciernen, y una vez conocido el contenido de éstas, si lo encuentra incompleto, no veraz, erróneo, "antiguo" o contrario al derecho, podrá solicitar su actualización y rectificación, siempre que la información haya sido recabada en bancos de datos y "*en archivos de entidades públicas y privadas*" en forma manual, mecánica, escrita o electrónica (informática)[3] . Conocimiento, acceso, actualización y rectificación de los datos personales del concernido que afecten al manejo, uso y control de la información de la persona, como a sus derechos fundamentales, principalmente al derecho a la intimidad personal y familiar y a su buen nombre.

La primera parte del inciso 1º del artículo 15 constitucional, establece en nuestro criterio una especie de *Hábeas Data administrativo*, si el concernido con los datos ejercita el derecho de petición (artículo 23, constitucional) y/o los recursos administrativos ordinarios o extraordinario previstos en el Código Contencioso-administrativo o C.C.A (artículos 49 y ss., y 69 y ss.,) para solicitar la aprehensión o acceso de los datos personales y lo hace ante una persona de derecho público de cualquier nivel administrativo (Nacional, Distrital, Departamental, Municipal y corregimental), ante una persona de derecho privado con función o servicio público (artículo 1º C.C.A.). Esto sin perjuicio de ejercer la "acción de tutela" ante los jueces individuales y autoridades, tribunales y Altas Cortes judiciales que forman parte de la jurisdicción constitucional colombiana y según los factores de competencia, ejercicio de la acción utilizado como mecanismo transitorio para defender o garantizar el derecho fundamental de petición, o bien ejercida directamente cuando se ha agotado previamente los mecanismos administrativos o jurisdiccionales pertinentes y no existe otro remedio jurisdiccional o administrativo para tutelar un derecho fundamental (artículo 86 constitucional y Decreto 2591 de 1991). Si se ejercita la acción de tutela en una de las dos formas para aprehender el conocimiento y/o acceso a la información o datos personales del concernido, decimos que emplea el *Hábeas Data jurisdiccional* en esta fase del tratamiento de datos.

Iguales reglas previas o concomitantes al ejercicio de la acción de tutela específica o de Hábeas Data, se podrá impetrar por parte de la persona concernida y/o afectada con los datos o informaciones inexactos, incompletos, erróneos, "antiguos", falsos o contrarios al ordenamiento jurídico vigente, cuando se persigue la actualización y rectificación de los mismos. En efecto, se interesado o afectado con los datos personales, podrá hacer uso del Hábeas Data administrativo si estima que más viable y expedito que el Hábeas Data jurisdiccional. Sin embargo, como profundizaremos más adelante al comentar los tipos de Hábeas Data en la doctrina, se ha impuesto en la praxis colombiana que la acción de tutela es la seleccionada por los colombianos para proteger y defender los derechos fundamentales incluidas las facultades del Hábeas Data de conocimiento, acceso, actualización y rectificación de la información o datos personales y se justifica como lo exige el Reglamento de la acción de tutela, que ésta se emplea como "mecanismo transitorio para evitar un daño irreparable"

---

(3) En la Obra hacemos una amplia explicación de los medios mecánicos y electrónicos, telemáticos o informáticos, utilizados en el tratamiento de datos personales, en la elaboración del Documento Electrónico –"*E-document*"-- y en la tipificación de los nuevas conductas delictivas sobrevenidas por la abusiva o ilegal utilización de las nuevas tecnologías de la información y la comunicación (medios TIC) y la informática. RIASCOS GOMEZ, Libardo O. ***La Constitución de 1991 y la Informática Jurídica***. Ed. UNED, Universidad de Nariño, Pasto, 1997, p. 10 y ss.

pese a existir otros mecanismos jurisdiccionales con igual finalidad [4].

En el inciso 2º del artículo 15, constitucional se refiere a las etapas o fases del tratamiento o procesamiento de datos, sean éstas realizadas con medios mecánicos o escritos, o bien con medios informáticos (electrónicos o telemáticos). Estas fases son: *la recolección, tratamiento y circulación de datos,* en las cuales como lo enfatiza la Constitución, *se res petarán la libertad y demás garantías consagradas en la Constitución*.

En el transcurso del tratamiento o procesamiento de datos personales, como profundizaremos *ut infra,* son viables el Hábeas Data administrativo como el Hábeas Data jurisdiccional y aquí con mayor razón, ya que son en éstas fases del tratamiento de datos donde se presenta la alta tensión, vulnerabilidad y/o defensabilidad y protección de los derechos y libertades fundamentales de la persona.

Cuando el artículo 20 constitucional, *garantiza a toda persona la libertad… de informar y recibir información veraz e imparcial…*" está garantizando un derecho universal [5] y un derecho incorporado al derecho nativo mediante las Ley 74 de 1968, por el cual se aprueba el Pacto internacional de derechos civiles y políticos y la Ley 16 de 1972, por el cual se aprueba el Convenio Americano sobre derechos Humanos o Pacto de San José de Costa Rica. En los artículos 19 y 13, respectivamente, se recogen el derecho, los deberes y las responsabilidades del Estado y los particulares respecto al derecho a la información, entendido éste en el más amplio sentido y no solamente en la especie aplicable al derecho periodístico, de "prensa" o de "imprenta". Se garantiza las dos visiones del derecho a la información: la activa de informar veraz, oportuna, completa y libre de errores o limitante o restricción alguna, salvo las estipulada en la Constitución y la ley y en cabeza del Estado o sus entidades, organismos o dependencias o de los particulares con función o servicio público; así como la visión pasiva de recibir información veraz, completa, imparcial, oportuna, eficaz y libre de limitantes y restricciones que no sean las autorizadas por el ordenamiento jurídico vigente.

Finalmente, el artículo 74, garantiza a *todas las personas* el derecho que ostentan *para acceder a los documentos públicos,* que interesen o afecte un derecho o libertad fundamental de una persona natural o jurídica y se hayan recabado en un banco de datos o archivo de una entidad pública o privada con función pública, o bien cuando dichos documentos estén involucrados en una cualquiera de las fases del tratamiento de datos personales.

El derecho de acceso a la información pública cualquiera sea la forma del almacenamiento o del tratamiento (mecánico, escrito o electrónico), garantizado a toda persona natural o jurídica se encuentra reglamentado con carácter pre y post constitucional a 1991, en la Ley 4 de 1913, artículo 32; en Ley 57 de 1985 o "Estatuto de la Información", el C.C.A.; la Ley 527 de 1999 (acceso electrónico a documentos o páginas de WEB públicos y privados) y la Ley 962 de 2005 o "Estatuto Antitrámites" en Colombia.

---

(4) "*LA TUTELA COMO MECANISMO TRANSITORIO.* Aún cuando el afectado disponga de otro medio de defensa judicial, la acción de tutela procederá cuando se utilice como mecanismo transitorio para evitar un perjuicio irremediable. / En el caso del inciso anterior, el juez señalará expresamente en la sentencia que su orden permanecerá vigente sólo durante el término que la autoridad judicial competente utilice para decidir de fondo sobre la acción instaurada por el afectado….(Artículo 8º del Decreto 2591 de 1991).

(5) El artículo 19 de la *Declaración Universal de los derechos Humanos* de 10 de Diciembre de 1948, por el cual "Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión".

La acción de tutela específica de Hábeas Data en Colombia desde su instauración en la Constitución de 1991, como segundo Estado de Latinoamérica e instituir y elevarla a rango constitucional, ha provocado en buena hora, un amplio y fructífero trabajo jurisprudencial de la Corte Constitucional como un mesurada labor de la doctrina especializada en pro de la estructuración, desarrollo, alcances, efectos jurídicos materiales y sustanciales y la evolución de la institución jurídico constitucional del Hábeas Data, tal como lo demostramos a lo largo de esta obra jurídica. Todo por cuanto, en nuestro país todavía no nace a la luz pública una ley que regule integralmente el derecho y garantía constitucional del Hábeas Data.

El Congreso de la República desde antes de la Constitución de 1991 y con mayor razón después de ésta ha avocado el conocimiento de diversos proyectos de ley ordinaria y de ley estatutaria que persiguen regular sectorial o parcialmente el derecho de Hábeas Data, sobre todo en algunas fases del tratamiento informatizado o no de datos personales, con énfasis en el dato financiero de carácter comercial, bancario, tributario y tarifario o de servicios públicos domiciliarios.

La Institución jurídico constitucional del Hábeas Data en Colombia, hoy por hoy, a pesar de haberse expedido la Ley 1266 de 2008, diciembre 31, por la cual se dictan "las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y proveniente de terceros países…", en todas aquellos otros datos personales no económicos o financieros, sigue siendo es una acción de tutela específica que *a priori* tiene las siguientes connotaciones: (i) La acción de tutela puede ejercerla toda persona que vea amenazado o vulnerado algún derecho o libertad fundamental; (ii) El Hábeas Data por la ubicación orgánica, denominación y clasificación en la Constitución *ab intio,* es un derecho fundamental [6], a tenor del artículo 86, constitucional; (iii) Es un derecho de aplicación inmediata, según el artículo 86, es decir, "*que no requiere previo desarrollo legislativo o de algún tipo de reglamentación legal o administrativa para su eficacia directa y que no contemplan condiciones para su ejercicio en el tiempo, de modo que son exigibles en forma directa e inmediata*" [7]; (iv) Como derecho fundamental el Hábeas Data, sí el legislador decide reglamentarlo sólo deberá hacerlo mediante una ley estatutaria (artículo 152-1, constitucional), cuya aprobación, modificación o derogación exigirá de la mayoría absoluta de los miembros del Congreso y deberá efectuarse dentro de una sola legislatura, según el artículo 153 ibíd. Además, requerirá del control de constitucional previo y automático de la Corte Constitucional sobre la exequibilidad del proyecto. Se aclara *in fine* del artículo citado que "*cualquier ciudadano podrá intervenir para defenderla o impugnarla"* [8]; (v) Es ejercita para garantizar y proteger los derechos fundamentales, incluidos la intimidad, el buen nombre, el honor, la información, el libre desarrollo de la personalidad, contra toda amenaza o vulneración por acción u omisión de las "autoridades públicas"; (vi) La protección efectiva de la tutela consistirá en la orden judicial que imparta el juez constitucional mediante sentencia para que el funcionario o autoridad pública actúe o se abstenga de hacerlo; (vii) La acción procederá cuando el interesado o per-

---

(6) "El derecho fundamental al habeas data, es aquel que otorga la facultad al titular de datos personales, de exigir a las administradoras de datos personales el acceso, inclusión, exclusión, corrección, adición y actualización, y certificación de los datos, así como la limitación en la posibilidades de divulgación, publicación o cesión de los mismos, conforme a los principios que informan el proceso de administración de bases de datos personales". Sentencia T-279 de 2002 de la Corte Constitucional.

(7) Sentencia T-002-1992 de la Corte Constitucional

(8) El trámite de varios proyectos de ley ordinaria del Hábeas Data posterior a la expedición de la Constitución de 1991 y hasta antes de la Sentencia C-008-1995 que declaró inconstitucional el proyecto No. 127/93 de la Cámara y No. 12 /93 del Senado, relativo a las fases del tratamiento de datos financiero, por no seguir el trámite especial de ley estatutaria, permitió vislumbrar el carácter de derecho fundamental regulado por ley estatutaria que el Hábeas Data tiene.

judicado no disponga de otro medio judicial, salvo que se utilice como un mecanismo transitorio para evitar un perjuicio irremediable; y, (viii) El Habeas Data origina un procedimiento sumario y preferente y sin mayores formalidades o ritualidades, adelantado a voluntad por la persona concernida o por quien lo represente.

2.2. Conceptualización de habeas data, titulares de los datos y los datos personales en el derecho comparado y la Ley 1266 de 2008

El objeto de la ley citada es "*desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en banco de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países*".

El habeas data en consecuencia es un derecho de rango constitucional circunscrito no sólo a los elementos de estructuración dados en forma explícita en el artículo 15 constitucional, sino en complementariedad con los artículos 20 y 74 de la Constitución, en definitiva tal como habíamos conceptualizado aún antes de la expedición de la ley.

La diferencia evidente del concepto dado al habeas data en la citada ley es la referencia excluyente de los datos financieros o económicos sobre todos los demás –que a propósito son muchos— que fue el objetivo primigenio y último de los proponentes de los proyectos de ley estatutaria (Congreso y Gobierno) que finalmente se convirtió en ley.

La presente concepción de habeas data está estructurada por una serie de elementos (i) el jurídico que incorpora la connotación de ser un derecho fundamental, autónomo y diferente a la intimidad, el buen nombre, el libre desarrollo de la personalidad y el de autonomía personal y el de información, aunque tengan identidades y tronco común como el valor de la dignidad de la persona humana; (ii) el estructural, constituido por unas acciones o verbos consecutivos: conocer, actualizar y rectificar informaciones o datos de la persona que le conciernen y hallan recolectados y almacenados en Bancos de datos o ficheros; (iii) el procedimental, constituido por las diferentes etapas del procedimiento por el que atraviesan los datos personales para llegar a ser cedidos, transferidos o puestos en circulación. Esas etapas son: la recolección, el tratamiento propiamente dicho y el almacenamiento en bases de datos; (iv) el ideológico, compuesto por el contenido mismo de los datos personales, su reserva, confidencialidad y disponibilidad según su connotación jurídica y entronque con otros derechos y libertades constitucionales.

Por tal razón, a continuación haremos una breve reseña de los datos personales y las diversas clasificaciones previstas en la Ley 1266 de 2009.

De la conceptualización generalizada del Hábeas data como derecho y como garantía constitucional, se puede deducir que los sujetos que intervienen en su estructuración están, de un lado, (i) los titulares de los datos, los causahabientes o sucesores, y de otro, (ii) El Estado como persona jurídica de derecho público y los responsables de los bancos de datos públicos o privados, o de "las centrales de información" financiera (crediticia, bancaria, bursátil, tributaria, tarifaria, etc.,) o especializada.

2.1.1. El Titular de los datos. El Hábeas Data en el ámbito latinoamericano es un derecho constitucional aforado a "*toda persona*" que tiene como facultades prioritarias, en principio el acceso y conocimiento de la información o datos personales que a ella le conciernen, y luego

según la aprehensión de este conocimiento, si observa que los datos son inexactos, incompletos, erróneos, "antiguos", falsos, "discriminatorios" o no conformes a derecho, podrá solicitar ante las personas, autoridades públicas o privadas, en vía administrativa o vía jurisdiccional, según el Estado latinoamericano y las reglas de competencia por éstos establecidas: la actualización, la rectificación, la eliminación o la "anulación" de los datos personales.

2.1.1.1. Las personas físicas, naturales o humanas. En el contexto de las Constituciones Latinoamericanas y las correspondientes leyes reglamentarias del derecho de Hábeas Data [9] en forma inequívoca se confiere la titularidad de los datos personales a toda persona, *ab initio*, natural, física o humana determinada o determinable, pues no cabe la titularidad de los datos para una persona anónima. La titularidad evoca un claro derecho de propiedad inmaterial sobre el dato, además de las facultades o derechos inherentes al Hábeas data: acceso, conocimiento, actualización, rectificación y eliminación datos personales recabados en bancos, registros, bases o ficheros de datos o informaciones personales, sean de naturaleza pública o privada.

2.1.1.2. Las personas jurídicas, morales o de "existencia ideal". Aunque en principio se discutió la titularidad de datos personales por parte de las personas jurídicas, morales o de "existencia ideal" (como se le denomina en el derecho argentino, uruguayo y del Paraguay), muy pronto se desistió de la tesis negativa, por las siguientes razones: (i) la persona jurídica, al igual que la persona física, es titular de derechos y obligaciones en el derecho universal; (ii) Los textos constitucionales y leyes latinoamericanas, al reglamentar la institución jurídica del Hábeas Data (como acción, recurso, garantía o proceso) lo hace recaer en "toda persona", como del titular de los datos personales, sin hacer distinción alguna sobre su naturaleza jurídica (humana o moral), el sexo, la nacionalidad, el domicilio e incluso la edad cronológica (desde el *nasciturus* por vía excepcional tendría titularidad en éste derecho); y, (iii) Aunque algunos derechos inherentes a la persona humana, como el de la intimidad por ejemplo, no serían los tutelados cuando se solicita la protección de datos de la persona jurídica, sí podría eventualmente solicitarse la tutela del derecho a la "*identidad o a la buena imagen*" porque en éste caso, "*el Hábeas Data protege un derecho a la verdad sobre los datos sociales que se posean en un determinado registro y que hagan a la reputación fama y buen nombre del afectado*" [10].

2.1.1.3. Personas humanas y jurídicas. Excepciones. La Ley Nacional de Protección de datos de la Argentina de 2000 en el artículo 2º, inciso 7º, y en similar sentido varias leyes Latinoamericanas sobre el particular, reconoce expresamente que es titular de los datos personales, "*toda persona física o persona de existencia ideal (o jurídicas) con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento de datos*". En cambio, la Ley No. 19.628 de 1999, relativa a la "protección de la vida privada o protección de datos de carácter personal", al prever como bien jurídico tutelado sólo a la privacidad o la intimidad de las personas, arroga la titularidad del derecho de Hábeas data a la persona física en el artículo 2º -ñ, así: "*Titular de los datos, la persona natural a la que se refieren los datos de carácter personal*" [11].

---

(9) RIASCOS GOMEZ, Libardo O. ***El habeas Data: Visión Constitucional, visión legal y en proyectos de ley estatutaria***. En http://akane.udenar.edu.co/derechopublico

(10) PALAZZI, Pablo. ***El Hábeas Data en el derecho argentino.*** Revista de Derecho Informático. ISSN 1681-5726. Ed. Alfa-Redi, No. 04, Noviembre de 1998.

(11) AA.VV. ***Ley sobre protección a la vida privada o protección de datos de carácter personal.*** En: http://www.sernac.cl/leyes/

Este proceder de la legislación Chilena es coherente porque la ley solo protege el derecho a la intimidad individual y familiar de las personas, al igual que lo siguen haciendo las leyes de protección de datos personales de Europa, tanto las nacionales (caso de España [12], Portugal, Francia, Alemania) como las comunitarias (Recomendaciones de OCDE y Convenio de Estrasburgo de 1980 y 1981, respectivamente y las Directivas 95/46/CE y 97/66/CE). En todas ellas el titular de los datos es el "afectado o interesado" con los datos personales, que sólo puede serlo la persona natural o física.

La Ley Federal Alemana de protección de datos de 1976-1994 o LFAPD, consecuentemente con lo anterior y al hacer mención a la persona humana como titular de los datos, en el "proceso" o tratamiento de datos, hace expresa referencia a los derechos derivados del acceso y consulta de la información. Estos derechos son: (i) La información acerca de los datos almacenados en relación con la persona; (ii) La Rectificación de los datos almacenados en relación con su persona, cuando los mismos fueren inexactos; (iii) El bloqueo de los datos almacenados en relación con su persona cuando no pudiere determinarse su exactitud o inexactitud, o cuando dejaren de darse las condiciones que originariamente requirieran su almacenamiento; y (iv) La cancelación de los datos almacenados en relación con su persona, si su almacenamiento no había sido admisible o bien --a elección, además del derecho de cancelación-- cuando dejaren de darse las condiciones que originariamente requirieran su almacenamiento.

Tanto las personas humanas como jurídicas están legitimadas para incoar una acción, recurso o garantía de Hábeas Data en un proceso jurisdiccional o administrativo, bien sea en forma directa, a través de apoderado judicial o mediante el representante legal de la entidad, organismo o dependencia pública o privada, según fuere el caso y clase de persona.

En los proyectos de ley estatutaria del Hábeas Data en Colombia, encontramos la corriente latinoamericana y no europea respecto de los titulares de los datos. En efecto, en el proyecto de Ley No. 64 de 2003, "*por el cual se dictan disposiciones para la protección de datos personales y se regula la actividad de recolección, almacenamiento y circulación de datos*", se determina que es "*Titular del dato personal…toda persona natural o jurídica, pública o privada a quien se refiere la información que reposa en un banco de datos o central de la información"*.

En sentido similar, el proyecto de ley estatutaria No. 071 de 2005 "por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera y crediticia, y se dictan otras disposiciones", cambia el término de "datos" por "información", para concluir diciendo que el "*Titular de la Información…Es la persona natural o jurídica, a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la…ley*". En idéntico sentido el último proyecto de Hábeas Data presentado al Congreso de la República en el año de 2006 y que hasta la fecha no se ha convertido en ley. Es el proyecto de Ley Estatutaria No. 211/2007 Cámara, No. 027/2006 Senado, acumulado con el No. 05/2006 Senado, "*Por el cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial y de servicios…"*

---

(12) **Afectado o interesado:** Persona física titular de los datos que sean objeto del tratamiento de datos respectivo, según la Ley Orgánica de protección de Datos No. 15 de Diciembre 23 de 1999 o LOPDP

Finalmente, El artículo 2º-a, de la Ley 1266 de 2008, reconoce que el titular de los datos o la información, *es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de habeas data y demás derechos y garantías a que se refiere la ley"*

2.1.1.4. El "afectado", "cualquier persona", las organizaciones con fines e intereses colectivos y el Defensor del Pueblo están legitimados para incoar el Hábeas data colectivo. En el derecho argentino se planteo la posibilidad de "*ejercer una suerte de Hábeas Data colectivo en los casos de discriminación*" [13] previsto en el inciso 2º del artículo 43 de la Constitución por parte del "*afectado, el defensor del pueblo y las organizaciones que propendan por esos fines*" (protección al ambiente, a la competencia, al usuario y al consumidor, así como a los derechos de incidencia colectiva en general).

Estos estarían legitimados por activa para proponer la acción de Hábeas Data en interés colectivo cuando en un banco o tratamiento de datos personales se amenace o vulnere un derecho fundamental con cualquier forma de discriminación.

En el derecho colombiano el proyecto de Ley estatutaria de Hábeas Data de 2005, a instancias de la Defensoría del Pueblo, mencionó por vez primera "*el Hábeas Data colectivo*" o "de interés público" ejercitable, según los artículos 3-4 y 24, por "*cualquier persona, organización o al defensor del pueblo",* para *"solicitar la suspensión, rectificación o cesación de un tratamiento de datos que se está realizando de manera irregular, con pretermisión de los requisitos establecidos para ello, o respecto de datos que no pueden ser objeto de tratamiento o cuyo tratamiento está sujeto a condiciones o requisitos que no se han cumplido y que afecta a una generalidad o grupo de personas determinadas o no"*. Habeas data colectivo que no puede interpretar o confundirse con las acciones de grupo o popular constitucional prevista en nuestra Constitución en el artículo 88 y reglamentada en la Ley 472 de 1998, pues aunque el fundamento de unas y otras son los derechos de la colectividad, "la generalidad" o la comunidad, el objetivo específico del Hábeas Data colectivo se dirige exclusivamente a restringir, limitar o prohibir un tratamiento o procesamiento de datos personales informatizado o no que amenace o vulnere derechos constitucionales o legales de esa colectividad.

2.1.1.5. "Curadores o tutores del afectado" y los causahabientes. La LPD Argentina de 2000, en el artículo 34, al mencionar la legitimación por activa de la acción de protección de datos personales o de Hábeas Data, sostiene que podrá ser ejercitada además del "afectado" o titular de los datos, por "sus curadores o tutores", es decir, por las personas elegidas o nombradas para cuidar los bienes o negocios de un menor de edad, o de quien no estaba en estado de administrarlos por sí.

El proyecto de ley estatutaria colombiana de Hábeas Data de 2005, a instancia de la Defensoría del Pueblo, preveía un trato jurídico especial para los menores de edad que estuviesen involucrados en un tratamiento o procesamiento de datos o más aún cuando ya estuvieren recabados en una base o banco de datos, pues en el artículo 7º manifestaba que "el tratamiento, uso, transmisión o divulgación de datos se asegurará el respeto a los derechos prevalentes de los niños"; agregaba en el inciso 2º , "El tratamiento de datos de carácter personal de menores sólo podrá hacerse con fines institucionales autorizados por la ley"; y finalizaba en el inciso 3º proscribiendo "el tratamiento, uso, divulgación, publicación o circulación de datos de carácter personal de menores cuyo fin sea su comercialización, tráfico, venta o cesión a terceros, excepto cuando se trate de información sobre solvencia patrimonial

---

(13) PALAZZI, Pablo. ***El Hábeas Data en el derecho…*** Ob., ut supra cit.

o financiera de menores adultos requerida en desarrollo de contratos de la misma índole para los cuales se encuentre habilitado por ley.

De lo anterior se deduce que en el evento que pudiese estar involucrado un menor de edad en un tratamiento o procesamiento de datos personales y con éste se afecte, amenace o vulnere derechos constitucionales o legales, éste como titular de los datos podrá a través de sus padres, o de su tutor o curador nombrado o designado al efecto, o mediante apoderado judicial, ejercitar la acción de Hábeas Data.

Respecto al término "causahabiente", utilizado por varias leyes Latinoamericanas de protección de los datos personales, o también reglamentaria del Hábeas data; así como en el proyecto de Ley Estatutaria colombiano de 2003 y 2007 de iniciativa de la defensoría pública y de origen gubernamental y parlamentario, respectivamente, lo hacen en el sentido lato o amplio, es decir, que causahabiente genéricamente se denomina a "cualquier persona que deriva el todo o parte de sus derechos de otra que se llama su "autor" o "causante". Si la derivación se verifica por un acto entre vivos se denomina transferencia y si se verifica por causa de muerte, transmisión, la que puede ser a título universal o a título singular.

De suerte, entonces, que son terceros relativos los herederos y legatarios de alguna de las partes y los cesionarios de ellas, todos los cuales son causahabientes.

Los sucesores o causahabientes reciben el derecho de su causante o autor en las mismas condiciones en que éste lo tenía, es decir, el derecho pasa de causante a sucesor con las mismas ventajas y cargas.

Los sucesores o causahabientes a título singular sufren los efectos de los actos realizados por su causante solo en relación con la cosa o derecho que se les ha transferido o transmitido.

Los sucesores o causahabientes a título universal, en cambio, les afectan todos los actos de su causante, todos los actos les aprovecha o perjudica; todos los derechos adquiridos por su autor, salvo los personalísimos; y deben cumplir todas sus obligaciones".

El proyecto de ley No. 064 de 2003, al definir al "titular de la información" manifestaba que ostentaba esta calidad la persona a la quien le conciernen los datos y "*sus causahabientes*" quienes *"gozan también de legitimidad para el ejercicio de los derechos y acciones correspondientes"* al Hábeas Data.

El Proyecto de Ley Estatutaria de 2007, sin mencionar expresamente en la definición de "titular de la información" a los causahabientes, en el contexto del proyecto hace referencia a los derechos que éstos tienen en todas las etapas del tratamiento o procesamiento de la información o datos personales, en las mismas condiciones y formalidades que los titulares de la información o datos. V.gr. en la "circulación de información", artículo 5º; así como también en el trámite del Hábeas Data administrativo colombiano, originado por peticiones, consultas o reclamos ante las autoridades de control o los responsables de los bancos de datos o "centrales de información" financiera o especializada (artículo 16 del proyecto).

De lo anterior se infiere entonces que los causahabientes son titulares de los datos por transferencia o transmisión de su autor o causante y por lo tanto, está legitimado por activa para ejercer los derechos o facultades del Hábeas Data.

2.1.2. El Estado. En el término más universalmente conocido, el estado es la persona jurídica de derecho público que puede adquirir derechos y contraer obligaciones. En tal virtud, los organismos, dependencias o entidades que hacen parte del estado en tal estén

representadas legal, estatutaria o legítimamente, podrán ser eventualmente titulares de datos que éstas les conciernan y estarán legitimadas para ejercitar algunas de las facultades o derechos componentes del Hábeas Data, pero obviamente no en defensa y protección del derecho a la intimidad como derecho personalísimo exclusivo de las personas naturales o físicas, como anteriormente hemos sostenido.

Estos organismos, entidades o dependencias del Estado están legitimados en esta clase de asuntos del Hábeas Data, tanto por activa como por pasiva, según si son titulares de los datos personales o por el contrario son responsables, administradores o manejadores de los bancos de datos públicos, o centrales de información financiera o especializada de carácter público.

Según *Palazzi* [14], al plantear la posibilidad de que el Estado sea "el actor en un proceso de Hábeas Data", será posible, "*cuando éste actúe en el campo del derecho privado. Pensamos que para que ello suceda, el Estado, o quien lo represente, debería estar registrado en un banco o base de datos, o al menos existir un determinado dato, o una información a la que se pretenda acceder*". Y agrega, "*Recordemos que el artículo 43 establece un derecho de acceso y control de la información que puede ser ejercido en forma independiente del derecho de rectificar o actualizar esa información*".

De esta forma, el autor citado parece plantear que el Estado sólo podría ejercitar las facultades del Hábeas Data de acceso y conocimiento de la información o datos y excluye las facultades de actualización, rectificación y cancelación de datos. Teóricamente es posible ejercitar todas las facultades del Hábeas data así sea el titular una persona jurídica.

2.1.2.1. Los responsables del tratamiento, banco o registro de datos, "Centrales de información" financiera o especializada, los "Operadores de los Datos", los fuente-operador de información y "Las Agencias de información comercial"

Las definiciones son sinónimas en el concepto de ser personas naturales o jurídicas, públicas o privadas que administran, manejan, dirigen o son responsables de los bancos de datos personales públicos o privados y constituyen se constituyen como "sujetos pasivos" del tratamiento informatizado o no de datos, en otros términos, son los sujetos legitimados por pasiva. Se diferencian, en atención al Estado donde se aplican dichas denominaciones, así como en algunas funciones especiales y en las leyes que les dan origen: unas, por las leyes de protección de datos; y otras, por leyes reguladoras del Hábeas Data integral, general o sectorial.

La Ley Orgánica de Protección de datos de España o LOPDP de 1999, en el artículo 3-d, define al "Responsable del fichero o tratamiento", como la "*persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento*".

En la definición se destaca la naturaleza y titularidad jurídica de las personas que realizan el tratamiento de datos personales y sobre todo la finalidad, contenido y uso del mismo.

En la legislación argentina, LPDA de 2000, se define al "*Responsable del archivo, registro, base o banco de datos", como la "persona física o de existencia ideal pública o privada, que es el titular de un archivo, registro, base o banco de datos*".

En esta definición se parte del sinónimo de archivo, registro, base o banco de datos entendido

---

(14) PALAZZI, Pablo. ***El Hábeas Data en el derecho…*** Ob., ut supra cit.

solo en el tratamiento informatizado o no de datos personales, para luego hacer énfasis en la titularidad pública o privada de dicho tratamiento y la persona que administra, dirige o es responsable de aquél.

Por su parte el proyecto de Ley estatutaria colombiana de Hábeas Data No. 064 de 2003, definía al "Responsable del tratamiento", como "*la persona natural o jurídica, pública o privada, o el servicio u organismo que trata datos personales por cuenta del operador del banco de datos o de la central de la información*". Se partía del ejemplo extranjero europeo y latinoamericano sobre el responsable del tratamiento de los datos o del "fichero" o banco de datos, para luego incorporar en dicha definición también a los denominados "operadores de los bancos o de la central de información". Esto por cuanto en Colombia son las organizaciones privadas con servicios financieros, como la "Central de Información" de la Asociación bancaria y de entidades financieras de Colombia –CIFIN-*, Data Crédito*, Covinoc, Computec, Inconcrédito, Credicheque, Fenalcheque, etc. "*sociedades o agremiaciones de carácter privado en las cuales se registra el comportamiento crediticio, financiero y comercial de las personas que celebran operaciones con entidades financieras, cooperativas y empresas de sector real* "[15] y son las que han dominado el mercado de la información crediticia y bancaria en Colombia, por varios años y las que han generado gran parte de la jurisprudencia de la Corte Constitucional en materia del dato financiero en nuestro país. En el derecho comparado coexisten entidades u organismos de información financiera de carácter privado con las de naturaleza pública (v.gr. En el derecho argentino "La Central de Deudores del Sistema Financiero" como sistema de información crediticia del Banco Central de la República Argentina, B.C.R.A)[16].

El proyecto de ley estatutaria colombiana de Hábeas Data sectorial de 2006 y 2007, la nominación de "responsables del tratamiento", "responsables de los bancos de datos", "responsables del tratamiento o bancos de datos por cuenta de un tercero: el operador" o los "responsables de las centrales de información" para unificarlos en uno sólo omnicomprensivo de todos los anteriores: "El Operador de la Información".

En efecto, en el artículo 3-c, del proyecto de ley define al "*Operador de información***"**, como "*la persona, entidad u organización que recibe de la fuente datos personales sobre varios titulares de la información, los administra y los pone en conocimiento de los usuarios bajo los parámetros de la presente ley. Por tanto el operador, en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos. Salvo que el operador sea la misma fuente de la información, este no tiene relación comercial o de servicio con el titular y por ende no es responsable por la calidad de los datos que le sean suministrados por la fuente*". Este concepto se plasmó finalmente en la Ley de habeas Data de 2008.

Los titulares de los datos o la información, entre otros derechos reconocidos por el proyecto de ley de 2006-2007, tendrán los siguientes derechos frente a los operadores de los bancos

---

(15) En: http://www.superfinanciera.gov.co/GuiasInformativas/educa-centralesriesgo.htm

(16) La central es un servicio de información del B.C.R.A, a través de la superintendencia de entidades financieras y cambiarias. Se ha estructurado en base a los datos que proveen las entidades financieras, las entidades no financieras emisoras de tarjetas de crédito y el propio B.C.R.A. Tiene por objeto brindar información sobre los deudores del sistema financiero a los bancos y demás instituciones que intermedian en el crédito, para facilitar la toma de decisiones en materia crediticia". LIVELLARA, Silvina. ***Hábeas Data e información crediticia. La eventual responsabilidad civil de las entidades financieras y del banco central de la República argentina por cesión y publicidad de datos inexactos.*** Vía Internet.

de datos: (i) Ejercer el derecho fundamental al hábeas data en los términos de la presente ley, mediante la utilización de los procedimientos de consultas o reclamos, sin perjuicio de los demás mecanismos constitucionales y legales; (ii) Solicitar el respeto y la protección de los demás derechos constitucionales o legales, así como de las demás disposiciones de la presente ley, mediante la utilización del procedimiento de reclamos y peticiones; (iii) Solicitar prueba de la certificación de la existencia de la autorización expedida por la fuente o por el usuario; (iv) Solicitar información acerca de los usuarios autorizados para obtener información. En idéntica forma se plasmo en la Ley 1266 de 2008 en el artículo 6º, sobre los derechos de los titulares de la información.

Se aclara sobre estos derechos que: (i) La administración de información pública no requiere autorización del titular de los datos, pero se sujeta al cumplimiento de los principios de la administración de datos personales y proyecto de ley; y (ii) La administración de datos semi-privados y privados requiere el consentimiento previo y expreso del titular de los datos, salvo en el caso del dato financiero y crediticio, el cual no requiere autorización del titular. En todo caso, la administración de datos semi-privados y privados se sujeta al cumplimiento de los principios de la administración de datos personales y a las demás disposiciones de ley. Estas aclaraciones quedaron plasmadas en el parágrafo único del artículo 6º de la Ley de Habeas Data.

2.1.2.2. Fuentes de Información y los "fuente-operadores" de información financiera. El artículo 3, literal j, de la Ley de Protección de datos personales de España, como norma integral del "Hábeas Data", se ocupa al igual que la LPDA argentina de 2000, principalmente por determinar las fuentes accesibles al público, las cuales las denomina como "*aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los Diarios y Boletines oficiales y los medios de comunicación*".

En cambio, el proyecto de ley estatutaria colombiano del Hábeas Data de 2006-2007 enfatiza en el concepto de fuente de información de carácter financiero, bien si actúa como tal o lo hace en forma sui géneris, como fuente-operador. En efecto, según el literal b, del artículo 3º del proyecto se entiende como "Fuente de información,… *la persona, entidad u organización que recibe o conoce datos personales de los titulares de la información, en virtud de una relación comercial o de servicio o de cualquier otra índole y que, en razón de autorización legal o del titular, suministra esos datos a un operador de información, el que a su vez los entregará al usuario final. Si la fuente entrega la información directamente a los usuarios y no, a través de un operador, aquella tendrá la doble condición de fuente y operador y asumirá los deberes y responsabilidades de ambos. La fuente de la información responde por la calidad de los datos suministrados al operador la cual, en cuanto tiene acceso y suministra información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstas para garantizar la protección de los derechos del titular de los datos*". Idéntico concepto quedó plasmado en la Ley 1266 de 2008, artículo 3-b.

Según el proyecto de ley estatutaria colombiana de Hábeas Data 2006-2007, el titular de los datos personales tiene los siguientes derechos frente a las fuentes de información: (i) Ejercer los derechos fundamentales al hábeas data y de petición, cuyo cumplimiento se podrá realizar a través de los operadores, conforme lo previsto en los procedimientos de consultas y reclamos de esta ley, sin perjuicio de los demás mecanismos constitucionales o legales; (ii)

Solicitar información o pedir la actualización o rectificación de los datos contenidos en la base de datos, lo cual realizará el operador, con base en la información aportada por la fuente, conforme se establece en el procedimiento para consultas, reclamos y peticiones; y (iii) Solicitar prueba de la autorización, cuando dicha autorización sea requerida conforme lo previsto en la presente ley. Estas derechos de idéntico tenor quedaron plasmados en el artículo 6º , numeral 2º de la Ley de Habeas Data Colombiana.

2.1.2.3. Las Agencias de Información Comercial. Excepciones normativas. En el literal i) del artículo 3º del proyecto de ley Estatutaria colombiana de 2006-2007, define a la "*Agencia de Información Comercial"* como "*toda empresa legalmente constituida que tenga como actividad principal la recolección, validación y procesamiento de información comercial sobre las empresas y comerciantes específicamente solicitadas por sus clientes, entendiéndose por información comercial aquella información histórica y actual relativa a la situación financiera, patrimonial, de mercado, administrativa, operativa, sobre el cumplimiento de obligaciones y demás información relevante para analizar la situación integral de una empresa. Para los efectos de la presente ley, las agencias de información comercial son operadores de información y fuentes de información*".

En el parágrafo de la norma citada, el proyecto de ley, aclara que a las agencias de información comercial, así como a sus fuentes o usuarios no se les aplicará, lo siguiente: 1. Los deberes que tienen las fuentes de la información, siguientes: ((i) Reportar, de forma periódica y oportuna al operador, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada; y (ii) Informar al operador que determinada información se encuentra en discusión por parte de su titular, cuando se haya presentado la solicitud de rectificación o actualización de la misma, con el fin de que el operador incluya en el banco de datos una mención en ese sentido hasta que se haya finalizado dicho trámite. 2. Lo relativo a la permanencia de la información, previsto en el artículo 13 del proyecto de ley; y 3. Lo referente al acceso a la información por parte de los usuarios, establecido en el artículo 15 del proyecto de ley.

Tanto la definición de "Agencia de Información Comercial", como las aclaraciones previstas en el parágrafo quedaron plasmadas en el artículo 3º , literal j., de la Ley de Habeas Data Colombiano.

2.1.2.4. Los Usuarios de la información. En particular, los "usuario-fuente". La LPDA de 2000, define al usuario de la información, como la "*persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos*".

La Directiva Comunitaria No. 95/46/CE, 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, entre las definiciones que incluye no regula al usuario de la información, sino a los "destinatarios" de la misma, porque entiende que éste puede ser una persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba "comunicación de datos", se trate o no de un tercero. Aclara la directiva, que las autoridades que reciban una comunicación de datos en el marco de una investigación específica no serán considerados destinatarios.

En el proyecto de ley estatutaria colombiano No. 064 de 2003, en el extenso catálogo de definiciones, sostiene que el "usuario o destinatario" de la información, es "*toda persona a quien se suministra la información contenida en un banco de datos o central de información, debidamente autorizada por el titular".*

Por su parte el proyecto de ley estatutaria colombiano de 2006-2007, sostiene que "usuario", sin más, es "*la persona natural o jurídica que, en los términos y circunstancias previstos en la presente ley, puede acceder a información personal de uno o varios titulares de la información suministrada por el operador o por la fuente, o directamente por el titular de la información. El usuario, en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos. En el caso en que el usuario a su vez entregue la información directamente a un operador, aquella tendrá la doble condición de usuario y fuente, y asumirá los deberes y responsabilidades de ambos"*.

En el fondo esta definición de usuario se apega al texto concreto y explicativo que traía la Directiva Comunitaria europea sobre los destinatarios de la información, el cual tenía derecho a la fase de comunicación de los datos, es decir, al acceso de la información. Sin embargo, el proyecto establece una connotación especial y por su puesto un régimen igualmente especial para los que denomina "usuario-fuente".

El proyecto de ley, regula con los derechos que tiene el titular de los datos frente a los usuarios de la información en general así: (i) Solicitar información sobre la utilización que el usuario le está dando a la información, cuando dicha información no hubiere sido suministrada por el operador; y (ii) Solicitar prueba de la autorización, cuando ella sea requerida conforme lo previsto en proyecto de ley.

Además los titulares de información financiera y crediticia, tendrán los siguientes derechos frente a los usuarios de la información: (i) Podrán acudir ante la autoridad de vigilancia para presentar quejas contra las fuentes, operadores o usuarios por violación de las normas sobre administración de la información financiera y crediticia; y, (ii) pueden acudir ante la autoridad de vigilancia para pretender que se ordene a un operador o fuente la corrección o actualización de sus datos personales, cuando ello sea procedente conforme lo establecido en la ley.

Tanto la definición de usuarios, como los derechos de los usuarios en general como aquellos que lo son de la información financiera y crediticia, quedaron plasmadas de idéntico tenor en el artículo 3º -d, y 6º -3 y parágrafo, respectivamente.

2.1.3. En el ámbito Latinoamericano: Datos o Informaciones personales. Diversa protección según la clasificación de los datos.

En el derecho latinoamericano, la definición de datos personales no solo se predica de las Personas naturales sino también de las personas jurídicas. En efecto, en la LPDA de 2000, los datos personales constituyen la "*información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables*", es decir, que incluye la información generada por las personas jurídicas, morales o de "existencia ideal".

En casi todas las leyes de protección de datos (Argentina), de protección a la vida privada (Chile), de acceso a la información pública y de transparencia de la gestión pública (Honduras), de protección al dato financiero (Uruguay); entre otras, contienen definiciones sobre los datos o informaciones personales, similares a las que trae la LPDA de 2000, la cual a su vez, retoma la definición y los parámetros conceptuales del derecho europeo. Por eso con la definición de la LOPD es prototípica.

Así mismo, la LPDA clasifica a los datos personales generales o simplemente "datos personales" y a los "datos sensibles" o pertenecientes al núcleo duro de la intimidad. Estos últimos se definen como aquellos "*datos personales que revelan origen racial o étnico, opiniones políticas,*

convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual".

En idéntico sentido regula la definición de datos sensibles la Ley Chilena No. 19.628 de 28 de Agosto de 1998, "sobre protección a la vida privada o protección de los datos de carácter personal" y la Ley No. 17938 de Octubre 1º de 2004 o "*Ley de protección de datos personales para ser utilizados en informes comerciales y el Hábeas Data*" del Uruguay.

2.1.4. En los proyectos de ley estatutaria y en la ley 1266 de 2008 sobre habeas data en el derecho colombiano.

En los primeros proyectos de leyes estatutarias del Hábeas Data Integral, general o en la mayor de las veces de carácter sectorial (hacia el dato financiero), posterior a 1995, se ha incluido en el capítulo definiciones las atinentes a los datos personales y los datos sensibles, siguiendo los cuadros normativos latinoamericanos, ya que en el derecho continental europeo, los "datos sensibles" son una categoría de datos surgida en los tratados o estudios doctrinarios de los juristas, más que en la plasmación de textos normativos, como hemos visto. A partir de 2002 y hasta Junio de 2007 en los proyectos de ley estatutaria, además de las definiciones de datos personales y datos sensibles se aumentaron otras tales como: dato negativo, dato público, dato privado y dato semi-privado que más adelante precisaremos.

Así por ejemplo, en el Proyecto de Ley estatutaria acumulado 201 de Cámara, 071 de 2002 de Senado, relativo a "*Por la cual se regula integralmente el derecho fundamental al habeas data y demás libertades y derechos fundamentales de las personas en lo que respecta al tratamiento de sus datos personales a través de bases de datos públicas y privadas, y se dictan otras disposiciones"* **[17]**, los ponentes introducen una definición de dato personal, ampliada a la del derecho europeo y el latinoamericano, al afirmar que éste es "*toda información relativa a personas físicas, jurídicas o de hecho que de cualquier manera sea idóneo para permitir, directa o indirectamente, su identificación tales como, entre otros, los nombres y apellidos, los números de identificación personal, los datos financieros, tributarios o de solvencia patrimonial o crediticia*". Se amplía en la cobertura de aplicación de la definición, pues se entiende a las "personas de hecho" y se incluye aspectos de identificación de las personas humanas y jurídicas, tanto de derecho público como de derecho privado.

También por inclusión de los ponentes, se define al "*dato sensible*", como "*aquel dato personal cuyo contenido involucra riesgos de prácticas discriminatorias por razones raciales y étnicas, opiniones políticas, convicciones religiosas, filosóficas o morales, la afiliación sindical, informaciones relacionadas con la salud, la vida* sexual o cualquier otra circunstancia similar de carácter personal o social". Y agrega en el inciso 2º: "*La recolección, almacenamiento, procesamiento, tratamiento, uso y suministro del dato sensible requerirá del consentimiento expreso, previo y escrito de su titular".*

El dato o "*información sensible*" como prefiere denominarla el proyecto, le asigna un plus de protección frente a los demás datos o informaciones personales. Este plus de protección está previsto en los artículos 4º y 27º así: (i) Se requiere el consentimiento, previo y escrito del titular del dato, si por excepción es sometido a tratamiento o procesamiento de datos; (ii) Nadie está obligado a proporcionar datos sensibles; (iii) Sin consentimiento pueden ser sometidos a trata-

---

(17) El intitulado del proyecto original era: "por la cual se regula el derecho de acceso a la información de interés público, en particular la de carácter comercial, financiero, la que tiene que ver con el cumplimiento de obligaciones fiscales y parafiscales y con el pago de servicios públicos domiciliarios, y se dictan otras disposiciones". Vid. HERNANDEZ, Jaime A. y VARGAS, Javier. ***Pliego de modificaciones al proyecto de ley Estatutaria 201 de 2003 y 071 de 2002 Senado***. Ponentes del proyecto acumulado. Vía Internet.

miento de datos, “cuando medien razones de interés general autorizados por ley” o cuando se persiga “finalidades estadísticas o científicas” y “no puedan ser identificados sus titulares”; y, (iii) Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revelen la identidad del titular de los datos sensibles. Sin perjuicio de ello, las iglesias, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros.

Por su parte, el proyecto de ley estatutaria del Hábeas Data No. 064 de 2003, a instancia de la Defensoría del Pueblo, en el artículo 5º, amplía aún más la definición del anterior proyecto, al sostener que “dato personal” es “*toda información relativa a personas físicas, jurídicas o de hecho que de cualquier manera sea idónea para permitir, directa o indirectamente, su identificación, tal como el nombre y apellidos, número de identificación personal, voz e imagen, o datos financieros, tributarios o de solvencia patrimonial y crediticia*”. La amplia en los identificadores de las personas físicas o naturales: voz e imagen; y mantiene en los de las personas jurídicas y de hecho.

En cuanto, al “dato sensible”, en el numeral 7 del artículo citado, lo define como “*aquel dato referido al origen racial o étnico, las opiniones políticas o filosóficas, las convicciones religiosas, la pertenencia a sindicatos o relativos a la salud o la sexualidad de una persona, cuyo tratamiento está proscrito por involucrar riesgo de prácticas discriminatorias*”. En esencia esta se mantiene la definición del proyecto anterior, pero se mejora en la redacción de la norma. El inciso 2º mantiene la esencia del consentimiento del titular con el nombre de autorización del titular de los datos, al decir: “*La recolección, registro, almacenamiento, procesamiento, tratamiento, uso y suministro del dato sensible sólo se hará en los casos y para los fines previstos en esta ley*”.

El dato sensible sigue siendo ultra protegido en todas las fases del tratamiento o procesamiento de datos personales, al punto que esta práctica se prohíbe por regla general (artículo 34) y solo por excepción se permite cuando el titular de los mismos otorga **“***autorización* (previa y escrita) *sólo para el tratamiento con fines históricos, científicos, estadísticos u otros de interés general previstos de forma expresa en la ley*”. Se refuerza, cuando dice: “ninguna persona está obligada a proporcionar datos sensibles” (artículo 67), salvo que “*medien razones de interés general autorizadas por la ley”* o para los fines anteriormente relacionados.

En el proyecto de Ley Estatutaria del Hábeas Data No. 071 de Cámara de 2005, que quizá sea uno de los más prolíficos en definiciones que se haya presentado al Congreso de la República, no solo suministra definiciones técnico-jurídicas aplicables al Hábeas Data, sino que las clasifica. Así dentro de las definiciones en “relación a la clasificación de los datos según su naturaleza” incluye: el dato personal, el dato público, el dato privado, el dato semi-privado y el dato íntimo, y en “otras clasificaciones”: “dato” y “registro individual.

Define como “*dato personal…cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley. Cuando en la presente ley se haga referencia a un dato, se presume que se trata de uno personal. Los datos personales pueden ser públicos, semiprivados o privados*”.

De esta definición se infiere las suministradas por separado como “dato” y “registro individual”, por lo cual se consideran innecesarias tales definiciones [18]. Ahora bien, se maneja una

---

(18) En el numeral 17 se manifiesta: “Dato: Es toda pieza individual de información contenida en los bancos de datos” y en el numeral 19, “Registro individual: Se refiere al conjunto de datos contenido en una base de datos relativo a un único titular de la información”.

definición amplísima de dato personal cuando se hace referencia a "cualquier pieza de información", aún cuando luego se refiera a la presunción que puede ser desvirtuada de dato solo referido a lo personal, pues si lo que se quería expresar es que la información, como se sostuvo anteriormente se concreta desde una manifestación informática binaria hasta un dato escrito o electrónico, auditivo, visual, audiovisual o telemático, estos no son "piezas" sino medios de crear, conseguir o recuperar información. Hoy conocemos medios escritos o tradicionales y medios electrónicos, telemáticos o informáticos [19]. En tal virtud, es universalmente entendible la definición que inicie sosteniendo "*cualquier información…"* referida a la persona física o jurídica.

El proyecto de ley, distingue entre dato sensible y dato íntimo, por vez primera para esta clase de normas, no sólo en el ámbito europeo, sino en el Latinoamericano.

En efecto, respeto al dato sensible lo define como "*aquel dato personal que puede potencialmente ser utilizado para discriminar a las personas, como es el relativo a la raza, la ideología o la orientación sexual*". Reduce, con relación a los anteriores proyectos de ley e incluso en lo pertinente a las legislaciones europeas y latinoamericanas, de una forma significativa el contenido del concepto de dato sensible a tres aspectos que pueden discriminar a la persona: la raza, la ideología o la vida sexual.

El dato íntimo, se considera "*el dato que, por su contenido o su naturaleza, las personas habitualmente prefieren mantenerlo en reserva y su conocimiento por parte de terceros no representa un interés general legítimo, como es el referido a los hábitos personales o a la vida familiar"*. Podría decirse que estos son los datos del círculo profundo de la vida privada a los que solo llega la misma persona y no representan alguna importancia o interés sino para su titular. Pese a que puede ser asimilable teóricamente el dato íntimo, es difícil distinguirlo de un dato anodino o superfluo para las demás personas pero para su titular de gran importancia y susceptible de tutela jurídica por el Estado. Por eso decíamos *ut supra* que en un dato anodino se puede esconder un dato personal o familiar, o viceversa y en ese hilo delgado de distinción se pueden cometer serias injusticias o desprotección estatal del derecho a la intimidad, al honor, al buen nombre, a la imagen, etc.

Por esto se considera innecesaria e inconveniente la definición suministrada. Sin embargo, el proyecto de ley para definir "el dato privado" toma como base las definiciones de dato sensible y dato íntimo. Sobre este aspecto más adelante profundizaremos.

Finalmente, el proyecto de ley estatutaria No. 221/2007 de Cámara y No. 027/2006 de Senado, acumulado con el No. 05/2006 Senado, "Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial y de servicios y se dictan otras disposiciones", en el artículo 3º relaciona unas definiciones técnico-jurídicas aplicables al

---

(19) Los medios escritos, documentales o tradicionales, son todos aquellos mediante los cuales se elabora, crea, modifica, archiva, procesa o destruye todo tipo de información no solo concerniente a las personas humanas o jurídicas, sino la referente a hechos, circunstancias, eventos no personales. En cambio, los medios electrónicos, telemáticos o informáticos, son aquellos mediante los cuales se trata o procesa información electrónica, con apoyo de las nuevas tecnologías de la información y la comunicación (TIC) y a través de software (programas de computador), hardware (equipos computacionales) y diversos elementos electro-magnéticos (Discos fijos y movibles, Discos compactos: CD, DVD, DI, etc., Disquetes; entre muchos otros.). El procesamiento electrónico de datos produce documentos electrónicos (El EDI anglosajón); bancos, bases, ficheros o registros electrónicos de datos de todo tipo, incluidos los bancos de datos personales, objeto y finalidad de leyes y proyectos de ley del Hábeas Data. Vid. RIASCOS GOMEZ, Libardo O. ***EL derecho a la Intimidad, la visión ius-informática y los delitos relativos a los datos personales.*** Tesis Doctoral, Universidad de Lleida (España), Lleida, 1999, p. 286 y 505

tratamiento o procesamiento de datos personales informatizados o no y en particular a las facultades o componentes del Hábeas Data, con énfasis financiero.

Este proyecto al igual que los anteriores prosigue con la distinción entre dato personal, dato público, dato semi-privado y privado, elimina la definición de dato íntimo y agrega la que llama *"Información financiera, crediticia, comercial, de servicios y la proveniente de terceros países".* Concordantemente con esto último, el catalogo de definiciones comienza con explicar qué debe entenderse por "titular de la información, y al efecto, dice: "*Es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la presente ley*".

El dato personal, según el literal e, del artículo 3º del proyecto, es "*cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley. Cuando en la presente ley se haga referencia a un dato, se presume que se trata de uso personal. Los datos personales pueden ser públicos, semi-privados o privados".*

La presente definición se mantienen los elementos suministrados en el proyecto 071 de 2005 y por tanto, son válidas para ésta las observaciones anteriormente realizada para éste proyecto.

Sobra haberse reiterado en la definición que no tienen sujeción al régimen jurídico del presente proyecto de ley estatutaria, los datos impersonales o no atribuibles a una persona determinada, o según el diccionario que "*no se aplica a nadie en particular*", pues según el intitulado y en el contexto del proyecto la ley se dice que rige para los datos personales o de la persona física o jurídica determinada o determinable. Estos datos impersonales tal como están excluidos de regulación podrían confundirse con los datos personales que han sido sometidos a procedimiento de disociación de manera que la información que se obtiene no puede asociarse a una persona determinada o determinable. Estos datos disociados son objeto de regulación por parte de la LOPDP española de 1999, los datos disociados a efectos de la comunicación (circulación, transferencia o cesión) de los datos son perfectamente posible sin necesidad de consentimiento y sin la previsión de derechos de cedente y cesionario (artículo 11º).

Por otra parte, parecería que no es dato personal la "*Información financiera, crediticia, comercial, de servicios y la proveniente de terceros países"*, que el proyecto de ley define en el literal j), del artículo 3º. Parecería decimos, porque *a renglón seguido de definir el dato personal dice que "pueden ser públicos, semi-privados o privados"* y excluye a propósito la información o datos financieros. Sin embargo, al emplear el término "pueden" se entiende que además de los mencionados en dicha definición caben otras posibilidades como la que mencionamos. Esto es de capital importancia para el proyecto de ley de Hábeas data sectorial, pues éste hace énfasis en el dato financiero.

Esta subespecie de dato personal se define así:

"*información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, aquella referida al nacimiento, ejecución y extinción de obligaciones dinerarias, independientemente de la naturaleza del contrato que les dé origen, así como la información relativa a las demás actividades propias del sector financiero o sobre el manejo financiero o los estados financieros del titular*".

2.1.4.1. El Dato semi-privado. El Proyecto de Ley Estatutaria No. 221/2007 de Cámara y No. 027/2006 de Senado, acumulado con el No. 05/2006 Senado, define al dato semi-privado, en el artículo 5º, literal g, como aquel dato "que *no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios…*".

Se define éste clase de datos por deducción lógica de lo que no es y por con el ejemplo aparentemente único del dato financiero que incluye al dato comercial, bancario, bursátil, tributario, fiscal o tarifario, como hemos sostenido anteriormente. Esta clasificación parecería estar mal informando al operador jurídico de la norma que es una especie de dato personal sui generis del cual es "propietario" su titular, pero no solo le interesa a él sino a "cierto sector o grupo de personas o a la sociedad en general", es decir, a todo el mundo, pero tan solo un poquito a él que paradójicamente es su titular concernido. Lo que no parece bien es que la norma al igual que lo hacía el centenario Código Civil Colombiano, explicaba las normas con ejemplos o casos ejemplarizantes (casuística). Esa técnica legislativa casi cerrada conlleva una pobre aplicabilidad general a diversos sucesos o eventos a los cuales podría estar dirigida.

En el proyecto de ley estatutaria No. 071 de 2005, se denominaba al dato semi-privado en la forma que lo hizo en el anterior proyecto, con la pequeña gran diferencia, que al final de la definición incorporaba aquello que en buena hora se eliminó en el año 2006-2007, es decir, que no se requería de "autorización del titular" para tratar o procesar esta especie de datos personales.

2.1.4.2. Dato privado. El Proyecto de Ley estatutaria No. 071 de 2005, define al dato en el artículo 5º, numeral 14, como aquel "*dato que por su contenido o su naturaleza sólo es relevante para el titular y no puede ser suministrado a terceros o usuarios, sino con su previa autorización. Son datos privados los datos sensibles y los datos íntimos. No podrá divulgarse o suministrarse un dato privado sin el consentimiento previo del titular, salvo las excepciones previstas en la ley*".

Esta calificación de dato privado encierra dos categorías especiales de datos que en el derecho continental europeo, como se dijo antes, tiene una protección reforzada porque implica nada más ni nada menos que los datos del famoso "núcleo duro" de la privacy anglosajona y por tanto, susceptible de máxima protección por parte del Estado. Así lo entendió el proyecto de ley de 2005, al imponer como requisito fundamental para tratar estos datos el consentimiento o autorización previa, expresa y escrita del concernido, sobre todo cuando se somete el dato a la fase de comunicación a terceros o usuarios.

Por su parte, el Proyecto de Ley Estatutaria No. 221/2007 de Cámara y No. 027/2006 de Senado, acumulado con el No. 05/2006 Senado, en forma aparentemente simple define en el artículo 5º literal h, al dato privado como aquel dato "*que por su naturaleza íntima o reservada sólo es relevante para el titular*". Es aparente, porque aunque elimina la calidad de dato sensible al privado le otorga otra candado de mayor seguridad que éste, cual es denominarlo como dato reservado. Y es la Constitución y las leyes especiales, como la Ley 57 de 1985, la que califica que es o no información reservada. Lo es por ejemplo, las investigaciones penales, las historias clínicas o médicas de una persona, etc.

Solo para ver hasta donde se extiende el concepto de dato privado, digamos lo siguiente:

Un ser humano desde antes de nacer, luego con su nacimiento, crecimiento, desarrollo, muerte, y aún después de ésta, produce una serie de actos, hechos, sucesos susceptibles de

documentación (certificados de cualquier tipo y finalidad, registros públicos y privados, obligaciones y contratos, etc.); en fin, de informaciones y datos personales, familiares y sociales, los cuales, en mayor o menor grado son sujeto u objeto del derecho y en mayores proporciones de la vida cotidiana, al ser puros y simples y reveladores de la venida, paso y extinción de la *vitae humanum*.

El status del *nasciturus* de la persona natural o física y el del *post mortem* en el derecho genera una gran cantidad de información o datos de carácter personal y familiar, tanto escritas, gráficas, auditivas, video auditivas como producidas, captadas, reproducidas, transferidas o consultadas por cualquier medio, dispositivo, aparato mecánico, eléctrico o electromagnético conocido o conocible, muchos de los cuales tienen relevancia en el derecho, dependiendo de diferentes variables que van desde las estrictamente biológicas (v.gr .nacimiento), pasando por las simplemente materiales u objetivas hasta las más sofisticadas que actualmente se conocen, cuando crean, modifican o extinguen situaciones jurídicas individuales o concretas, o generales y abstractas, produciendo derechos, deberes y obligaciones para una persona. Una auscultación médica mediante la técnica de rayos X o cualquiera otra de índole computarizada (p.e. TAC) o de examen de líquidos humanos (orina, sangre, semen, etc.) o incluso de partes del cuerpo humano (v.gr. huellas digitales o plantares); cualquier número o símbolo que identifique o se le asigne a una persona (v.gr. documento de identidad personal, profesional, documento de conducción, etc.); la información sobre la raza, origen étnico, color, religión, edad o estado civil o sobre la educación, su historial laboral, delictivo, incluso las ideas u opiniones personales sobre otra persona, salvo las vertidas con ocasión de un concurso, premio o subvención según la *Act Privacy Canadiense*; entre muchas otras relacionadas en un gran listado que no distingue categorías especiales entre aquéllas, constituyen información personal, entendiendo como tal, la que le concierne a una persona, cualesquiera sean los mecanismos o tecnologías de las que se obtengan o graben.

2.1.4.3. Información financiera, crediticia, comercial, de servicios y la proveniente de terceros países. Según el literal j, del el Proyecto de Ley Estatutaria No. 221/2007 de Cámara y No. 027/2006 de Senado, acumulado con el No. 05/2006 Senado, se "*entenderá por información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, aquella referida al nacimiento, ejecución y extinción de obligaciones dinerarias, independientemente de la naturaleza del contrato que les dé origen, así como la información relativa a las demás actividades propias del sector financiero o sobre el manejo financiero o los estados financieros del titular*".
Las definiciones de datos personales como las de dato público, privado y semiprivado quedaron plasmadas en la Ley 1266 de 2008, en el artículo 3º , literales e, f, g y h.

2.1.4.3.1. Actores del Habeas Data Financiero: Según el artículo 3º de la Ley 1266 de 2008, relacionaremos lo que se entiende por Titular de los datos, Fuentes de Información, Operadores de Centrales de Datos, Usuarios.

a) Titular de la información. Es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la presente ley;

b) Fuente de información. Es la persona, entidad u organización que ***recibe o conoce datos*** personales de los titulares de la información, en virtud de una relación comercial o de servicio o de cualquier otra índole y que, en razón de ***autorización legal*** o del titular, suministra esos datos a un operador de información, el que a su vez los entregará al usuario final. Si la fuente entrega la información directamente a los usuarios y no, a través de un operador, aquella tendrá la doble condición de fuente y operador y asumirá los deberes y responsabilidades de ambos. La fuente de la información responde por la calidad de los datos

suministrados al operador la cual, en cuanto tiene acceso y suministra información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstas para garantizar la protección de los derechos del titular de los datos;

c) Operador de información. Se denomina operador de información a la persona, entidad u organización ***que recibe de la fuente datos personales*** sobre varios titulares de la información, ***los administra y los pone en conocimiento de los usuarios*** bajo los parámetros de la presente ley. Por tanto el operador, en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos. Salvo que el operador sea la misma fuente de la información, este no tiene relación comercial o de servicio con el titular y por ende no es responsable por la calidad de los datos que le sean suministrados por la fuente.

2.1.4.3.2. Principios de Administración de datos Financieros. Según el artículo 4º de la Ley 1266 de 2008, los principios que rigen en la administración de los datos, es decir, en el desarrollo, interpretación y aplicación de la presente ley, se tendrán en cuenta, de manera armónica e integral, los principios que a continuación se establecen:

a) Principio de veracidad o calidad de los registros o datos. La información contenida en los bancos de datos debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el registro y divulgación de datos parciales, incompletos, fraccionados o que induzcan a error;

b) Principio de finalidad. La administración de datos personales debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley. La finalidad debe informársele al titular de la información previa o concomitantemente con el otorgamiento de la autorización, cuando ella sea necesaria o en general siempre que el titular solicite información al respecto;

c) Principio de circulación restringida. La administración de datos personales se sujeta a los límites que se derivan de la naturaleza de los datos, de las disposiciones de la presente ley y de los principios de la administración de datos personales especialmente de los principios de temporalidad de la información y la finalidad del banco de datos.

Los datos personales, salvo la información pública, no podrán ser accesibles por Internet o por otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o los usuarios autorizados conforme a la presente ley;

d) Principio de temporalidad de la información. La información del titular no podrá ser suministrada a usuarios o terceros cuando deje de servir para la finalidad del banco de datos;

e) Principio de interpretación integral de derechos constitucionales. La presente ley se interpretará en el sentido de que se amparen adecuadamente los derechos constitucionales, como son el hábeas data, el derecho al buen nombre, el derecho a la honra, el derecho a la intimidad y el derecho a la información. Los derechos de los titulares se interpretarán en armonía y en un plano de equilibrio con el derecho a la información previsto en el artículo 20 de la Constitución y con los demás derechos constitucionales aplicables;

f) Principio de seguridad. La información que conforma los registros individuales constitutivos de los bancos de datos a que se refiere la ley, así como la resultante de las consultas que de ella hagan sus usuarios, se deberá manejar con las medidas técnicas que

sean necesarias para garantizar la seguridad de los registros evitando su adulteración, pérdida, consulta o uso no autorizado;

g) Principio de confidencialidad. Todas las personas naturales o jurídicas que intervengan en la administración de datos personales que no tengan la naturaleza de públicos están obligadas en todo tiempo a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende la administración de datos, pudiendo sólo realizar suministro o comunicación de datos cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.

3. ORIGEN JURISPRUDENCIAL DEL HABEAS DATA EN COLOMBIA

Haremos mención a dos sentencias definitorias del Habeas Data en Colombia: (i) La T-552-1997, y (ii) La T-729-2002.

3.1. La Sentencia T-552-1997, el deslinde del derecho fundamental de habeas Data. Como comprobamos en la parte primera de esta Obra, al hacer la evolución jurisprudencial del derecho a la Intimidad, la Corte Constitucional en sus pronunciamientos comienza a deslindar el llamado "derecho de autodeterminación informática o informativa" del derecho a la intimidad personal y familiar de las personas. Esta labor se verifica en la Sentencia ***T-552-1997***, en donde la Corte Colombiana retomando los planteamientos jurisprudenciales vertidos por el Tribunal Constitucional Español en la famosa Sentencia 254 de 1993 (STS 254/93), sobre datos personales de un ciudadano que no había dado su consentimiento para que se recogieran y almacenaran en un base de datos de carácter público, se le desconoció su derecho a la autodeterminación informática o "libertad informática", prevista en el artículo 18-4 de la Constitución Española de 1978 (CE). Esta sentencia a su vez, se basó en los planteamientos de la sentencia de inconstitucionalidad de la Ley de Censo ciudadano proferida por el Tribunal Federal Alemán de 1983, la cual fundada en el derecho al libre desarrollo de la personalidad y la autonomía individual, concluyó que la ley transgredía las normas jurídicas constitucionales porque reglamentaba demasiados aspectos o datos personales, extralimitaba dicha función al relacionar informaciones de la persona más allá de las simples de empadronamiento, como son los datos de la vida íntima, sobre la propiedad, el ámbito comercial o financiera, de salud, etc., Esto hizo que el Tribunal alemán hablara por vez primera del derecho "*de autodeterminación informática o informativa*" o primigenio "habeas data", en Latinoamérica.

En efecto, la sentencia T-552-97, aunque por otras razones y fundamentos fácticos y jurídicos sostiene: *a pesar de que en determinadas circunstancias el derecho a la intimidad no es absoluto, las personas conservan la facultad de exigir la veracidad de la información que hacen pública y del manejo correcto y honesto de la misma. Este derecho, el de poder exigir el adecuado manejo de la información que el individuo decide exhibir a los otros, es una derivación directa del derecho a la intimidad, que se ha denominado como el derecho a la "autodeterminación informativa".* Se propone así, el derecho de autodeterminación informática devenido del derecho a la intimidad, pero aplicable a todas aquellas informaciones o datos de la persona que se desconocen por las entidades bancarias o financieras en sus relaciones eminentemente comerciales de crédito y ahorro privado. Esto porque es innegable que el derecho de habeas data en Colombia surge principalmente en el ámbito de sentencias de tutela sobre datos de carácter bancario o financiero.

En el presente caso, se trata de un particular que tutela a entidad bancaria (Granahorrar), por desconocimiento del derecho de habeas data, intimidad, Buen nombre entre otros, al desconocer la entidad el contrato de compraventa celebrado por el tutelante y la compradora y constituir en dicho contrato una hipoteca de primer grado para garantizar la deuda contraída

por él inicialmente. La compradora no registró la escritura ante la Oficina de Instrumentos Públicos, como era su obligación hacerlo, dentro del término de ley, y al no hacerlo, la entidad bancaria, reportó a ASOBANCARIA por la deuda inicial contraída al primer deudor que seguía apareciendo en la base de datos del banco, pues la obligación contraída con el banco no se había satisfecho en su totalidad por la no cesión de la obligación y su formalización jurídica, a través del registro de la escritura de compraventa con hipoteca de primer grado constituida por el deudor original y la adquirente del inmueble y la deuda mediante hipoteca a favor del banco granahorrar.

La mentada sentencia deslinda el derecho de habeas data, recogiendo a su vez, planteamientos jurisprudenciales anteriores sobre el tema.

Tal fue el sentido de las providencias SU-082/95 y T-176/95 que establecieron lo siguiente: "El contenido del **habeas data** se manifiesta por tres facultades concretas (…):
"a) El derecho a conocer las informaciones que a [las personas] se refieren; b) El derecho a actualizar tales informaciones, es decir, a ponerlas al día, agregándoles los hechos nuevos; c) El derecho a rectificar las informaciones que no correspondan a la verdad." (Sentencia SU-082/95). "Para que exista una vulneración del derecho al habeas data, la información contenida en el archivo debe haber sido recogida de manera ilegal, sin el consentimiento del titular del dato (i), ser errónea (ii) o recaer sobre aspectos íntimos de la vida de su titular no susceptibles de ser conocidos públicamente (iii)." (Sentencia T-176/95)

El derecho al habeas data es, entonces, un derecho claramente diferenciado del derecho a la intimidad, cuyo núcleo esencial está integrado por el derecho a la autodeterminación informativa que implica, como lo reconoce el artículo 15 de la Carta Fundamental, la facultad que tienen todas las personas de "*conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.*"

3.2. La sentencia T-729-2000, proporciona autonomía al Habeas Data. Se define el Habeas data y los datos personales, principios en el proceso informático, la protección a la información, los datos personales y su administración. En el caso concreto se tutela "*el derecho al habeas data o a la autodeterminación informática"* a una persona a quien se publican y revelan datos personales en diversos webs oficiales distritales, sin consentimiento del concernido. Actor solicita se le tutelen los derechos fundamentales de habeas data, intimidad, buen nombre entre otros, por cuanto el Departamento Administrativo de Catastro del Distrito y un Empresa de Seguridad Social Distrital al conformar una base de datos personales incluyó una serie de datos patrimoniales, personales y familiares que eran consultables en la internet, tan solo con el número de cédula. Al revelar datos de esta naturaleza que no fueron solicitados o consentidos por el interesado en la recolección, almacenamiento y posterior procesamiento y consulta de los mismos, se viola el derecho de habeas data o de "autodeterminación informativa o informática". La Corte ordena tutelar el derecho de habeas data, pues estima que las entidades debieron recibir el consentimiento del concernido para recoger, almacenar y difundir vía internet la información persona del tutelante. No se vulnera la intimidad en este caso, según la Corte.

4. TIPOS DELICTIVOS CONTRA LOS DATOS PERSONALES Y EL HABEAS DATA

4.1. ACCESO ABUSIVO A UN SISTEMA INFORMATICO

4.1.1. Fuente Normativa: Artículo 269 A. El presente delito hacía parte del Titulo VII del Titulo X., de C.P., del 2000, bajo el bien jurídico tutelado de la Intimidad y la reserva en las comunicaciones. Sin embargo, mediante la Ley 1273 de Enero 5 de 2009, que reformó

parcialmente el Código y creó el Titulo VII bis, intitulado de *los delitos contra la Información y los datos*, traspuso el artículo 195 al artículo 269 A, aunque algunos juristas interpretaron que se había derogado por dicha ley y nuevamente creado bajo el nuevo bien jurídico protegido.

La trasposición de tipos penales es una forma que utiliza el legislador para reubicar tipos que considera en su momento no están correctamente ubicados bajo dicho bien jurídico protegido y espera que bajo el nuevo que se ubique adquiera mayor potencialidad en la protección del bien jurídico y mayor punibilidad porque atenta a un bien jurídico más sensible.

También se aplican en este tipo penal básico las siguientes normas: (i) Ley 1266 de 2008, o ley de habeas data. Conceptualización, entre otros términos del habeas Data, Titular de la información, Dato personal, Dato público, Dato privado, Dato Semi-privado, usuario, fuente de información, "Agencia de Información Comercial", autoridades de vigilancia de los datos económicos (Superintendencia Financiera y Superintendencia de Industria y Comercio, Habeas Data administrativo y Habeas Data jurisdiccional;

(ii) Convenio de Budapest del Consejo de Europa de 23 de Diciembre de 2001, sobre Ciberdelincuencia, sobre conceptualizaciones de Sistema Informático, datos informáticos, proveedor de servicios, datos sobre el tráfico. Además, sobre acceso ilícito, interceptación ilícita, interferencia en los datos, interferencia en el sistema, abuso de los dispositivos. Sobre los delitos informáticos en particular: Falsificación informática, Delitos de relación con el contenido, delitos relacionados con infracciones de la propiedad intelectual y de derechos afines, entre otros. Se relaciona también aspectos procesales, conservación rápida de datos informáticos almacenados, conservación y revelación parcial rápidas de datos sobre el tráfico, registro y confiscación de datos informáticos, obtención en tiempo real de datos informáticos, etc. Sobre Cooperación internacional: principios generales: (i) Relativos a la extradición, (ii) asistencia mutua, y (iii) información espontánea. Finalmente, sobre procedimiento relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables.

4.1.2 Tipo penal. 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 1000 salarios mínimos legales mensuales vigentes.

4.1.3 Sujeto activo: El tipo penal Acceso abusivo a un sistema informático no requiere cualificación del agente, por lo que puede ser sujeto comisivo del delito un particular o un servidor del Estado. Sin embargo, si se comente por un funcionario estatal el tipo se agrava de conformidad con el artículo 269H-2 del C.P.

Hay que aclarar que esta clase de ilícitos pueden ser cometidos por cualquier persona particular o por un "usuario" en términos de la Ley 1266 de 2008 o ley de Habeas Data. Usuario que lo haría sin el consentimiento del titular del dato o violando la medidas de seguridad de los datos adoptados por el operador de la información o el fuente-operador de la misma, no solo la clave de acceso (Password) sino los elementos de seguridad interna del software o hardware, respectivamente.

Usuario en términos de la ley, es "*aquella persona natural o jurídica que, en los términos y circunstancias previstas en la ley, puede acceder a información personal de uno o varios titulares de la información suministrada por el operador o por la fuente, o directamente por el titular de la información. El usuario en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos. En caso en que el usuario a su vez*

entregue la información directamente al operador, aquella tendrá la doble condición de usuario y fuente, y asumirá los deberes y responsabilidades de ambos".

Por su parte el Convenio de Budapest de Diciembre 23 de 2001, manifiesta que "proveedor de servicios", se entenderá: (i) toda persona pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar por medio de un sistema informático, y (ii) cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios de ese servicio".

El Sujeto pasivo en esta clase de conductas es el Estado, pero también lo podrán ser las personas jurídicas o privadas que operen, administren o coordinen un sistema informático o base de datos cualquiera sea su finalidad, perfil o clase de banco de datos.

4.1.4. Conceptualizaciones necesarias para entender el tipo penal

En la conducta penal sobre conceptualizaciones tomaremos como norma extrapenal la ley 1266 de 2008 o ley de habeas data financiero y la terminología provista por el Convenio de Budapest de 2001, como referente doctrinal al no haberse incorporado al derecho interno colombiano mediante ley.

En efecto, Dato personal "*es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica*" (artículo 3, e, de la Ley de Habeas Data). Ahora bien si ese dato personal ingresa a un tratamiento o sistema informático, se convertirá en dato informático. El Convenio de Budapest de 2001, en su artículo 1º define a los datos informáticos, como **"***cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado que un sistema informático ejecute una función".*

Las propuestas legislativas que cursaban en el Senado de la República previas a la Ley 1273 de 2009 que adicionó el C.P. , con el título VII bis e incluyo nueve conductas delictivas y trasladó a éste título denominado "*de los delitos contra la información y los datos*", el acceso abusivo a un sistema informático, traían un artículo 1º dedicado a las definiciones técnicas y relativas a los medios TIC que se utilizan en los artículos 269 A a 269 I y que ayudaban a la comprensión terminológica de cada conducta penal en el trámite final de la ley 1273 fue eliminado, entendiendo equívocamente que esa labor pertenecía a la Corte Constitucional o a los Tribunales y jueces en el momento de aplicabilidad de la norma específica. Aunque eso es parcialmente cierto, no debemos olvidar que en nuestro país, respecto del fenómeno informático, electrónico y telemático muy poco se ha reglamentado con carácter ius civilista o administrativista o de *prima ratio* en donde se explique los varios términos tecnológicos TIC utilizados en las normas y se aplique una legislación pedagógica, preventiva y civilista a los variados casos permeados por las nuevas tecnologías de la comunicación y la información, así cuando ésta no funcione o funcione indebidamente se llega a una legislación penal o de *última ratio* y no al contrario como está sucediendo actualmente al leer la Ley 1273 de 2009.

Pues bien, uno de tantos proyectos de ley previos a la 1273, definían como ***sistema informático*** *todo dispositivo aislado o conjunto de conectores interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa de ordenador.*

Mediante un sistema informático se pueden almacenar, procesar, registrar o transmitir datos personales o informáticos bien se encuentren en un mismo o en diferentes sitios geográficos, pues el sistema involucra software y hardware que permite desde almacenar hasta transmitir información datos sean estos informáticos, electrónicos o telemáticos. Un sistema informático

podría estar interconectado a otro sistema informático, según las posibilidades de interconexión facilitadas por los diferentes dispositivos y que la tecnología lo permita o viabilice.

Esto significa que en un sistema informático, puede presentarse un acceso ilegal total o un acceso ilegal parcial, siempre que se vulnere una medida de seguridad, una contraseña, password (palabra o frase secreta de acceso a un sistema o base de datos) o clave de acceso, o bien se vulnere el acceso a una base o banco de datos.

4.1.5. Bien Jurídico Tutelado. La Ley 1273 de 2009, de enero 5, adicionó el C.P. del 2000 con el *Título VII bis* denominado de "la protección de la Información y de los datos" , que constituye a su vez, en el bien jurídico protegido en éste aparte del Código Penal. El Titulo está conformado por dos capítulos, a saber: (i) De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos; y (ii) de los atentados informáticos y otras infracciones". Cada uno de los cuales contiene varias conductas delictivas.

El delito de acceso abusivo a un sistema informático (artículo 269 A), pertenece al primer grupo de conductas delictivas y atenta a la confidencialidad de la información (el secreto o sigilo de la información) puesto que las actividades dolosas, ya que no admite formas culposas, van dirigidas al acceso ilegal o ilegítimo de los datos, la información o un sistema informático, en una primera acción instantánea, o bien a mantenerse dentro de un sistema informático contra la voluntad de su legítimo usuario del sistema o titular de los datos.

Antes de la adición del C.P., de 2000, la conducta delictiva de acceso abusivo a un sistema informático se hallaba localizada bajo el bien jurídico protegido de la Intimidad, el secreto a la correspondencia y las comunicaciones en el artículo 195 con una redacción parecida a la del artículo 269 A, pero se diferenciaba principalmente en lo siguiente: No especificaba cómo y de qué forma se podía acceder a un sistema informático, si era o no con autorización (aunque esto está implícito en la conducta penal, pues si es con autorización deviene la atipicidad del delito), y la sanción era apenas de multa lo cual no se compadecía con la insidiosidad del tipo.

El artículo 195 del C.P. del 2000, manifestaba: *"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"*.

El artículo 2º de la Ley 1273 de 2009, derogó expresamente el artículo 195 y en su lugar trasladó su contenido esencial del tipo al artículo 269 A, bajo el bien jurídico de "la información y los datos" personales, tal como se lo ha transcrito anteriormente.

Mediante la Ley 1288 de 2009 de Marzo 25, el Congreso de la República modificó algunas penas para varios delitos del Código Penal del 2000. En efecto en el artículo 25, se modificó la pena de multa del artículo 195 delito de acceso abusivo a un sistema informático, por pena de prisión de cinco (5) a ocho (8) años, todo por cuanto al dictarse dicha ley perseguía "*fortalecer el marco legal que permite a los organismos, que llevan a cabo actividades de inteligencia y contrainteligencia, cumplir con su misión constitucional y legal, y se dictan otras disposiciones*". El Capítulo V de dicha ley regula todo lo atinente a la *reserva de información en inteligencia y contrainteligencia* de los organismos del Estado que llevan a cabo dichas actividades. Según el artículo 3º de la mentada ley son: *las dependencias de las Fuerzas Militares y la Policía Nacional reglamentados por estas para tal fin; el Departamento Administrativo de Seguridad (DAS) y la Unidad de Información y Análisis Financiero (UIAF). Estos cumplen su función a través de operaciones básicas y especializadas, utilizando medios humanos o técnicos. Estos organismos conforman la comunidad de inteligencia y son los*

únicos autorizados para desarrollar labores de inteligencia y contrainteligencia en el ámbito de la seguridad y la defensa nacional.

En tal virtud, al modificar esta ley un tipo penal que estaba derogado previamente por la Ley 1273 de 2009, queda vigente el artículo 269 A, que de alguna forma había mejorado la redacción del artículo 195 y había establecido una sanción más acorde con el nivel insidiosidad estructurado en el tipo, pues la sanción pasó de multa a *prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 SMLMV*.

En tan pocos años de existencia de la conducta delictiva, el tipo penal ha cambiado de bien jurídico protegido, tanto solo por la ubicación probablemente más acorde con los denominados doctrinalmente "delitos informáticos" contra la información y los datos personales que por una de las tantas formas de vulnerar la intimidad de las personas o de la familia, a través de s visión iusinformática, como ut supra explicábamos.

4.1.6. La confidencialidad de la información. La ley1266 de 2008 o ley de habeas data, expone como principio fundamental de la administración de los datos personales el de confidencialidad, junto al de veracidad o calidad de los registros o datos, el de finalidad, de circulación restringida, temporalidad de la información, de interpretación integral de derechos constitucionales y el de seguridad.
Respecto a la confidencialidad, expresa que *todas las personas naturales o jurídicas que intervengan en la administración de datos personales que no tengan la naturaleza de públicos están obligadas en todo tiempo a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende la administración de datos, pudiendo sólo realizar suministro o comunicación de datos cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma* (artículo 3º , literal g).

La confidencialidad, reserva o sigilo de la información es por lo tanto un principio rector en el acceso, procesamiento, manejo, administración y transmisión de datos personales. Constituye la regla general en el tratamiento informatizado ("o automatizado") o no de la información perteneciente al ser humano que solo por excepción y bajo los apremios de ley, por autoridad competente (en nuestro país, la judicial) y para fines específicos (según el artículo 15 de la Constitución colombiana, para adquirir pruebas judiciales, para tasación tributaria e intervención estatal) podrá excepcionarse dicha confidencialidad o secreto.

La docente universitaria *Castro Ospina* [20], al explicar las razones que le asisten para defender la postura del bien jurídico protegido de *la Información* por el Código Penal de 2000, sostiene que la confidencialidad… *en nuestra sociedad moderna, (en) la comunidad tiene derecho a la privacidad de los datos atinentes a la vida personal de sus miembros; a las estrategias comerciales, publicitarias o mercantiles; a los secretos industriales; y a las comunicaciones; entre otras. Este derecho se traduce en un sentimiento de seguridad y de tranquilidad en la convivencia social.* Con lo cual hoy por hoy, la información de las personas o los datos del ser humano individual o familiarmente considerado en el mundo actual y en sus diferentes facetas del quehacer social, laboral, empresarial, educativo, profesional, etc., está permeada por el principio universal de la confidencialidad en aras de una convivencia pacífica, segura y alta civilidad. La autora citada dentro de un largo listado de Conductas que lesionan la confidencialidad de la información, siguiendo al tratadista *Reyna Alfaro,* expone las siguientes: **1) *El espionaje informático*** (industrial y comercial) y dentro de ellos las siguien-

---

(20) CASTRO OSPINA, SANDRA J. ***La información como bien jurídico y los delitos informáticos en el nuevo Código Penal Colombiano.*** Universidad Externado de Colombia, Bogotá, Julio 15 de 2002. Vía Internet.

tes conductas: (i) *fuga de datos (Data leake),* (ii) *puertas falsas (Trap Doors),* (iii) las *"llaves maestras" (Superzapping)*, (iv) *el pinchazo de líneas (Wiretapping)* y (v); *la apropiación de informaciones residuales (scavenging)* [21]*;* y, (ii) *El Intrusismo Informático*, es decir, la mera introducción a sistemas de información o computadoras, infringiendo medidas de seguridad destinadas a proteger los datos contenidos en ellos. Precisamente este segundo tipo penal es el que el Código Penal reformado en 2009, denomina acceso abusivo a un sistema informático, pues las conductas integrantes al espionaje informático nuestro C.P., lo tiene regulado bajo otro bien jurídico protegido del Orden Económico social y en el delito de "violación a la reserva industrial y comercial" (artículo 308) y cuyos medios comisivos comprenderían los informáticos, electrónicos o telemáticos (artículo 58-17 C.P., circunstancias de mayor punibilidad. Adicionado por el artículo 2º de la Ley 1273 de 2009).

Sin embargo, varias de las conductas aplicadas al espionaje industrial y comercial, son perfectamente válidas no sólo para ejemplificar el acceso abusivo a un sistema informático, sino para los demás tipos delictivos previstos en los artículos 269 B a 269 i, como anotaremos en su momento oportuno.

4.1.7. Nomen Iuris Universal. El acceso ilícito a un sistema informático, a una base, fichero o banco de datos en línea o fuera de ella, a un programa de computador (software) o un grupo de interconectores de información, ha sido considerado como un tipo básico de *intrusión informática*, aunque en los diferentes países afecte bienes jurídicos protegidos distintos**.** En efecto, en Colombia inicialmente afectaba a la Intimidad y la reserva de las comunicaciones (Ley 559 de 2000), y ahora al bien jurídico de la información y los datos (Ley 1273 de 2009). En España, se ubica como un tipo penal que afecta a la Intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio (C.P. Español de 1995).

El Convenio de Budapest de 2001, que rige para los Estados Miembros de la UE, pero con claro ejemplo para el resto de Estados del mundo, regula el "Acceso Ilícito" a sistemas informáticos, ficheros o registros informáticos, en línea o fuera de ésta, haciendo énfasis en que la figura delictiva tipificada en los ordenamientos internos debe considerar que ésta puede cometerse bien "*infringiendo medidas de seguridad (Códigos, claves, contraseñas, filtros, etc.) con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático*".

En la obra de Mitnick [22], nos muestra el mundo de los Hackers, que son aquellas personas

---

(21) ***El Espionaje informático***, debe entenderse, en términos de la doctrinante citada, "con ánimo de lucro y sin autorización, de datos de valor para el tráfico económico de la industria o comercio dentro de los comportamientos que encajarían en esta descripción, han sido identificados los siguientes: ***fuga de datos (Data leake),*** que las empresas o entidades guardan en sus archivos informáticos; ***puertas falsas (Trap Doors),*** consistentes en acceder a un sistema informático a través de entradas diversas a las que se utilizan normalmente dentro de los programas; las ***"llaves maestras" (Superzapping)***, que implican el uso no autorizado de programas con la finalidad de modificar, destruir, copiar, insertar, utilizar o impedir el uso de los datos archivados en los sistemas de información; ***el pinchazo de líneas (Wiretapping),*** que se concreta en interferir las líneas telefónicas o telemáticas, mediante las cuales se transmiten las informaciones procesadas; ***la apropiación de informaciones residuales (scavenging),*** que consiste en la obtención de información a partir de lo que desechan los usuarios legítimos de un sistema informático.

(22) MITNICK, Kevin, SIMON, William L. ***El arte de la intrusión. Cómo ser un hacker o evitarlos.*** Editorial Alfaomega Ra-ma, 1ª ed., 2007. El autor del libro es uno de los Hackers más famosos de Estados Unidos, detenido varias veces por sus actividades intrusivas en los sistemas informáticos más seguros. En base a su vida se han hecho películas como "Takedown" en 2000 que relata su última detención en 1995 y su puesta en libertad en 2002. Actualmente Kevin como muchos otros Hackers es reconvertido a ser consultor de compañías a quienes les ayuda a mejorar los sistemas de seguridad. Su compañía ***Mitnick Security*** anteriormente ***Defensive Thinking.***

que acceden, ingresan o actúan de forma intrusiva en los sistemas informáticos, bases o ficheros de datos en red o fuera de ella, y lo hace por el solo hecho de transgredir las normas de seguridad informática y demostrarse a sí mismo y sobre todo a los demás que las medidas que impiden el ingreso a un extraño a un sistema de seguridad no es confiable, es altamente vulnerable y su fácil intrusión es casi un juego de niños. A esta clase de intrusos el autor los califica de "*White Hacking*" **[23]**, por oposición diríamos nosotros a los "*Black Hacking*" que son aquellos intrusos en redes, sistemas o programas informáticos que además de buscar logros de envanecimiento personal van tras oscuras intensiones o con finalidades ilícitas, o provecho económico, financiero o de cualquier otro tipo en el que el intruso obtenga beneficio ilícito.

4.1.8. Verbos rectores alternativos (acceder-mantener). Conductas de ejecución instantánea y de permanencia**.**

El acceso abusivo a un sistema informático previsto en el artículo 269 A del C.P., se entiende a todos aquellas acciones que no están incluidas en el artículo 257, referidas al acceso ilegal o prestación ilegal de los servicios de telecomunicaciones, al menos en su parte inicial referida al acceso ilegal a los servicios de telecomunicaciones como los de telefonía móvil celular "u otro servicio de comunicaciones". Este ilícito se encuentra el Titulo VII de los delitos contra el patrimonio económico, Capítulo VI, sobre las defraudaciones.

Como se dijo antes el acceso ilícito a todo sistema informático incluye tanto los informáticos, electrónicos o telemáticos y por supuesto la telefonía celular o fija se encuadraría dentro de los medios electrónicos. Sin embargo, el acceso ilegal que reprime el artículo 257 se refiere más a la intrusión en el servicio de telecomunicaciones con algún fin o provecho, que al acceso ilegal vulnerando medidas de seguridad por demostrar su capacidad y vulnerabilidad del sistema, tal como lo hacen los hackers, o bien para mantenerse en el sistema contra la voluntad del que tiene derecho legitimo a excluirlo. Sin embargo, una y otra conducta delictiva es intrusiva aunque las finalidades sean distintas y recaigan sobre medios electrónicos.

Según el Convenio de Budapest de Diciembre 23 de 2001, previene a cada Estado miembro sobre el acceso ilícito, para que adopte medidas legislativas para evitarlo y que eleve a categoría de delitos el acceso deliberado o ilegítimo total o parcialmente. El acceso puede cometerse ya sea infringiendo "*medidas de seguridad*", para obtener datos informáticos o con otro fin delictivo, o en relación con un sistema que esté conectado a otro sistema informático.

Por su parte, referente a los "abusos de los dispositivos", la comisión deliberada o ilegítima podría darse en los siguientes actos:

1) La producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de: (i) un dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos de acceso ilícito, interceptación ilícita, interferencia en los datos o interferencia en el sistema; (ii) una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático, con el fin de que sean utilizados para la comisión de cualquiera de los delitos mencionados anteriormente.

2) La posesión de alguno de los elementos contemplados en los anteriores apartados, con el fin de que sean utilizados para cometer cualquiera de los delitos previstos anteriormente.

El fenómeno tecnológico TIC permanentemente evoluciona pues esa es la dinámica que le

---

(23) **Hacking:** Procedimiento mediante el que se violan los códigos personales y/o el acceso a datos o sistemas informáticos sin autorización y/o conocimiento del titular.

imprime no sólo el mercado, los usuarios y proveedores, sino que por esencia las nuevas tecnologías tienen que estar continuamente reinventándose a sí misma por que la obsolescencia deviene en espacios de tiempo cada vez más insignificantes. Obsérvese como alguien adquiere un equipo de computación de última generación, versión última y no han transcurrido algunos instantes, cuando sale la versión 2, luego 2 A y así sucesivamente, tal parece que ni siquiera el mercado puede estar al "*último grito*" de la moda, modelo, generación, versión o acápite de esa versión, porque simplemente la tecnología es apabullante y continuamente reactualizada.

Esa angustia de reinvención constante, permanente y penetrante es transmitida al mundo jurídico que no estabiliza tipos, figuras o conductas delictivas realizadas con medios informáticos, electrónicos o telemáticos, por la complejidad evolutiva de la tecnología y las altas capacidades humanas de utilizarlos indebida o ilegalmente más que en forma legítima o acomodada al derecho. Pudiese ser exagerado pero puede acercarse a la realidad decir que mientras las actuaciones ilícitas crecen en forma geométrica, las legítimas crecen en forma aritmética, pese a los continuos sistemas, redes o programas informáticos protegidos por alta tecnología de seguridad. Mientras haya puertas habrá quienes las traspasen.

Pues bien, ya cursan en el Parlamento varias propuestas de reforma el sui generis Capítulo VII bis de los delitos contra la "*información y los datos*" personales, no sólo sobre el articulado, los tipos penales establecidos, el cambio de punición, la mejor utilización del lenguaje para la estructuración de los tipos penales básicos y agravados; sino la eliminación, refundición o aumento de tipos penales que engloben mejor el bien jurídico protegido, para que no siga apareciendo como un bien jurídico difuso o "*intermedio* [24] *o de referencia individual*", como lo tildan juristas extranjeros como Ricardo M. Mata y Martín, citado por Castro Ospina.

Una de esas propuestas de reforma que referenciamos es el proyecto de ley que cursa en la Cámara de Representantes y en la que se reviven las definiciones técnicas aplicables a los diferentes tipos penales relativos a la protección de la información y los datos personales, entre otros, el acceso abusivo a un sistema informático. Dicha conceptualización es necesaria y coherente en una norma iuscivilista o iusadministrativista, pero no en una de carácter penal, al menos en la parte especial del Código Penal, pues todo lo aplicable a un código punitivo con carácter general o sectorial debe ir en la parte general del Código, para efectos de aplicabilidad y de sistematización temática y referencial.

Respecto, de la propuesta de esta conducta delictiva que todavía no ha tenido aplicabilidad práctica visible en los estrados judiciales colombianos y menos aún de revisión de los organismos jurisdiccionales techo en materia penal (Corte Suprema de Justicia), formalmente con incidencia en el fondo de la conducta típica del acceso abusivo en un sistema informático, se ha planteado lo siguiente:

Mejorar la redacción del tipo a fin de evitar la estructuración de conductas en blanco y evitar la

---

(24) Bienes jurídicos intermedios son "aquellos intereses colectivos tutelados penalmente de forma conjunta con bienes particulares, siendo ambos de carácter homogéneo o estando situados en la misma línea de ataque". Este tipo de bienes jurídicos son: (i) Suprapersonales, es decir que superan los intereses particulares, (ii) Están vinculados a un bien jurídico netamente personal; (iii) Pertenecen a los intereses de la comunidad y no al ámbito de los intereses del Estado, pues los primeros tienen una mayor relación con los bienes individuales; (iv) Son cualitativamente homogéneos con los intereses individuales que pueden resultar vulnerados; o se encuentran en una misma dirección de ataque del comportamiento punible; (v) Hay relación medial entre el bien colectivo y el bien individual; (vi) La lesión del bien jurídico intermedio representa un riesgo potencial para un número plural e indeterminado de víctimas; y (vii) La lesión al bien colectivo, como límite mínimo, no ha menoscabado de manera efectiva los bienes personales, que es el límite máximo. De esta forma se sobrepasa el estadio del peligro abstracto". Ob., ut supra cit., p. .4.

ambigüedad, falta de precisión terminológico-técnica a la hora de su aplicación a los casos concretos. Con ese objetivo se solicita la eliminación de los siguientes elementos normativos que se consideran innecesarios y ofrecen confusión: "*o por fuera de lo acordado", "en todo en parte", "protegido o no" y "legítimo"* utilizado en la redacción del tipo.

Aunque no contamos con la exposición de motivos de dicho proyecto, estamos de acuerdo con el planteamiento por las siguientes razones: (i) El término utilizado al inicio del tipo para cualificar el acceso a un sistema informático, "sin autorización o por fuera de lo acordado", resulta ambiguo no sólo "o por fuera de lo acordado", sino los mismos términos "sin autorización", pues se entiende que el acceso con autorización atipifica el tipo penal y por lo tanto sobraría la expresión que hoy tiene y se mantiene en la reforma propuesta. El término "por fuera de lo acordado", supone un convenio, acuerdo o contrato previo entre el que accede a un sistema informático y el usuario, lo que lo convertiría en un típico abusador de un sistema informático, pero eso también sobra porque quien accede a un sistema informático para encasillarse en la figura penal debe necesariamente no tener autorización de acceso alguna (v.gr. claves, contraseñas, permisión de acceso en ciertas horas, días, meses o medidas de tiempo de servicio del sistema), pues de lo contrario la atipicidad de la conducta sería plausible.

El término "en todo o en parte", utilizado para indicar el nivel de acceso a un sistema informático, interpretamos es innecesario pese a que el Convenio de Budapest de 2001, utiliza unos términos similares para indicar que se debe punir el "acceso deliberado e ilegítimo ***a la totalidad o a una parte de un sistema informático***". Es irrelevante cuantificar si el acceso a un sistema informático sólo se hace a una parte o a la totalidad del sistema, porque lo que determina la configuración del tipo es el acceso mismo, violando las medidas de seguridad el sistema, e incluso también es irrelevante si el acceso se considera deliberado (voluntario o hecho a propósito), si es ilegítimo (pasar por legítimo quien no lo es) o abusivo (Usar mal, excesiva, injusta, impropia o indebidamente de algo), pues la configuración de la conducta punitiva, tal como está prevista en la parte general del Código debe ser típica, antijurídica y culpable y por su puesto el acceso a un sistema se entiende que es ilegítimo, deliberado, abusivo o ilegal, de lo contrario devendría la atipicidad penal pero podría surgir configuración de una contravención especial o una infracción civil o administrativa según el grado de insidiosidad que tenga la conducta y eso sí es probable en nuestro sistema jurídico, a pesar de no haber normativización al respecto.

El término "legítimo", utilizado por la norma es innecesario porque la persona que tiene derecho a excluir el acceso o rechazar que permanezca en un sistema informático se entiende que es legítimo o conforme a derecho, pues de lo contrario no tendría facultad alguna de no permitir el acceso o rechazar la permanencia en el sistema. Eso pasaría con los operadores o fuentes de información específica que administran, controlan, vigilan o prestan servicios de consulta de información relevante en una base o fichero de datos en línea o fuera de ella. Estos administradores de la información tienen derechos y deberes que cumplir en el funcionamiento de esos sistemas informáticos y uno de ellos es precisamente es el "*permitir el acceso a la información únicamente a las personas que, de conformidad con lo previsto en la ley, pueden tener acceso a ella*" (artículo 7º de la Ley 1266 de 2008 o ley de Habeas Data financiera). Por su parte el titular de la información tiene sus derechos y deberes y uno de éstos frente a los operadores de los bancos de datos es: "*solicitar información acerca de los usuarios autorizados para obtener información*" (art 6-1º Ibíd.).

Finalmente, se propone la inclusión de los términos " o con otra finalidad ilícita" para denotar que el acceso a un sistema informático puede tener la "finalidad de obtener datos informáticos o con otra finalidad ilícita". Consideramos innecesario también el elemento normativo adicionado a la redacción de la conducta penal, aunque esa directriz la propone el Convenio

de Budapest de 2001 en el artículo 2º, al ejemplarizar que "el delito se comete infringiendo medidas de seguridad, con intención de obtener datos informáticos o ***con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático"***.

Si bien la reforma aclara que el acceso a un sistema informático es para "obtener datos informáticos" que no lo hace el actual artículo 269 A del C.P., pues sólo la punición deviene del acceso mismo a un sistema informático, entendiendo que es no solo por violar las medidas de seguridad para demostrar su experticia en las nuevas tecnologías de la información y comunicación ("White hackers") sino que implícitamente conlleva unas finalidades ilícitas que buscan algún provecho o beneficio para el agente o un tercero ("Black Hackers") de lo contrario, solo en la obra literaria del "Arte de la Intrusión" de Mitnick, es creíble que los que los hackers reconvertidos ahora en asesores de medidas de seguridad a sistemas informáticos altamente sensibles para la seguridad y defensa de los Estados, o para salvaguardar información relevante financiera, económica, industrial, intelectual, etc., solo lo hagan por la vanagloria personal, por el anonimato del pirata informático o por el voyeurismo informático, pues detrás de cada acción humana está una reacción que algún efecto produce desde los más nimios o anodinos hasta los más complejos e intrincados o incluso a veces inexplicables.

4.2. DELITO DE OBSTACULIZACION ILEGITIMA DE SISTEMA INFORMATICO O RED DE TELECOMUNICACIONES

4.2.1. Fuente Normativa: Art. 269 B. En esta conducta también son aplicables las normas extrapenales siguientes:

(i) Ley 1266 de 2008 sobre el Habeas Data, pues se requieren las conceptualizaciones previstas en aquella norma sobre sistema informático y datos informáticos y dentro de esta última los términos titular de la información, dato personal, dato privado, dato público, dato semi-privado o financiero, así como usuario, fuente y operador de la información y finalmente, los principios que rigen a la administración de la información, sobre todo el de seguridad y de confidencialidad de la información;

(ii) La ley 1288 de 2009, marzo 5, relativo al fortalecimiento del marco legal que permite a los organismos, que llevan a cabo actividades de inteligencia y contrainteligencia en el Estado colombiano para la seguridad y defensa nacional, puesto que toca con aspectos de acceso a información reservada por servidores públicos;

(iii) La Ley 1341 de 2009 de Julio 30 "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones —TIC—, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones". Especialmente sobre el entendimiento de las nuevas tecnologías de la información y la comunicación o TIC (*son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios, que permiten la compilación, procesamiento, almacenamiento, transmisión de información como voz, datos, texto, video e imágenes,* según el artículo 6º); el uso permitido, inspeccionado y controlado por el Estado a través del Ministerio de tecnologías de la Información y la comunicación o MinTIC y la Comisión de regulación de Comunicaciones (CRC) y la Agencia Nacional del Espectro (ANET), que es la competente para imponer sanciones a la vulneración del espectro electromagnético (artículos 63 y 64 Ibidem, excepto la previstas en el artículo 76, constitucional); así como también, los principios que rigen en las TIC, tales como que, *el derecho a la comunicación, la información y la educación y los servicios básicos de las TIC. En desarrollo de los artículos 20 y 67 de la Constitución Nacional el Estado propiciará a todo*

colombiano el derecho al acceso a las tecnologías de la información y las comunicaciones básicas, que permitan el ejercicio pleno de los siguientes derechos: La libertad de expresión y de difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, la educación y el acceso al conocimiento, a la ciencia, a la técnica, y a los demás bienes y valores de la cultura.

4.2.2. El Tipo penal. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

4.2.3. Sujetos de la conducta punible: Será sujeto activo una persona sin calificación alguna y por lo tanto puede ser un particular o un servidor del Estado. Solo que en éste último caso la sanción se agravará por así contemplarlo el artículo 269 H-2, como una circunstancia de agravación punitiva si la conducta se comete por un "servidor público", la pena se aumentará "de la mitad a las tres cuartas partes".

El sujeto pasivo podrá ser el Estado, pero también las personas jurídicas o particulares con o sin funciones públicas que administren, manejen, coordinen un sistema informático, bases o ficheros de datos.

4.2.4. La confidencialidad y disponibilidad de la información. La conducta no sólo afecta a la confidencialidad (el secreto o sigilo) de la información puesto que las acciones comisivas también incluyen el acceso a la información que se halla recolectada o almacenada en una base de datos o sistema informático, sino también a la disponibilidad de la misma, porque las acciones comisivas del agente se extienden hasta impedir u obstaculizar el uso, manejo, fluidez o transmisión de los datos personales o informaciones, lo cual impide el ejercicio normal y corriente de los derechos que le asiste al titular de la información, tales como el derecho a la intimidad, el habeas data, el de información misma, el buen nombre e imagen, entre otros personalísimos y sociales. "*La colectividad tiene derecho a la disponibilidad de la información sin perturbaciones ni trabas, pues ella les permite ejercer libremente sus derechos. Solo el conocimiento hace posible la libertad"* **[25]**

4.2.5. Conceptualizaciones. El Convenio de Budapest de 2001, en su artículo 1º define a los datos informáticos, como **"***cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado que un sistema informático ejecute una función".*

El dato personal entendido como "*cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que pueden asociarse con una persona natural o jurídica*" (según el artículo 3,e de la Ley 1266 de 2008), constituye una especie del dato informático que lo contiene y aunque la legislación nacional no lo estipule en los términos del Convenio de Budapest, uno de los proyectos de ley previos a la expedición de la Ley 1273 de 2009, sí lo hizo en el artículo 1º referido a las definiciones previas a la descripción puntualizada de las conductas punitivas que hoy conocemos insertas en el Capítulo VII Bis del C.P.

---

(25) **CASTRO OSPINA, S.J.** Ob., ut supra cit. 4. La autora cita como medios comisivos de los delitos contra disponibilidad de la información, las "bombas lógicas y los virus", pues argumenta que "transitoriamente (afecta) a la disponibilidad de la información sin destruirla. Otros son los "***Spam o el electronic-mail bombig***" que consiste en el envío de cientos o miles de mensajes de correo electrónico, no solicitados o autorizados, para bloquear a los sistemas.

La definición que traía el mentado proyecto, sostenía que el dato informático estaba constituido por "*cualquier representación de hechos, informaciones o conceptos de una forma que permita su tratamiento digital*". En esencia este concepto es igual al provisto por el Convenio de Budapest, pero es desafortunado por la mutilación que se hace de la última parte la definición del proyecto de ley, pues los términos "tratamiento digital" es omnicomprensivo del tratamiento informático, electrónico o telemático, antes todo lo contrario estos últimos tratamientos de la información sí contienen al "tratamiento digital". En todo caso, lo que significa el dato informático es que es una unidad de información cualquiera (personal, económica, financiera, política, científica, etc.) visual, auditiva, telemática, digital, encriptado, numérica o alfanumérica.

4.2.6. Verbos Rectores alternativos: Impedir, Obstaculizar. La Comisión del delito de obstaculización ilegítima de un sistema informático o red de telecomunicaciones se configura por los verbos impedir u obstaculizar el funcionamiento o el acceso "normal" (el termino es innecesario y ambiguo, cara a la antijuridicidad del tipo penal) a un sistema informativo, a los datos informáticos allí contenidos, o una red de telecomunicaciones.

Quien impide u obstaculiza el funcionamiento o el acceso de un sistema informático, a los datos allí contenidos o a una red de telecomunicaciones queda inmerso en la figura penal del artículo 269 B. Quien impide u obstaculiza el funcionamiento o el acceso al sistema informático, los datos o redes de telecomunicaciones necesariamente es quien accede a un sistema informático (tipo penal del artículo 269 A), pues no se puede impedir u obstaculizar el funcionamiento de un sistema informático, sí previamente no ha vulnerado los sistemas de seguridad del sistema informático para ingresar al mismo. Es una consecuencia, del ingreso el impedimento u obstaculización del sistema informático, por ello, bien pudo el legislador establecer un tipo delictivo general que prevea las diferentes fases del procedimiento o tratamiento de datos desde la recolección, selección, almacenamiento hasta el registro, comunicación y transmisión de datos [26] y en cada una de esas fases establecer los diferentes tipos penales que pudieren erigirse, cara a acceder, impedir, obstaculizar, interrumpir, interferir, bloquear, cancelar, destruir, dañar, interceptar, etc., el procedimiento informático.

Por eso, se nos ocurre que todas las conductas que afecte el procedimiento informático deberían comenzar en el actual delito de *"violación de datos personales", bases de datos, sistemas y procedimientos informáticos o redes de comunicación e información.* Y dentro de aquel comenzar en el primero inciso con la conducta del artículo 269F (Violación de datos personales" e informáticos); luego en el segundo, con el tipo del artículo 269 A (Acceso abusivo a un sistema informático); en el tercero con el tipo del artículo 269 B ("Obstaculización ilegítima a un sistema informático" se eliminaría a "red de telecomunicaciones"); en el cuarto con el tipo penal del artículo 269 C (Interceptación de datos informáticos); y en el quinto con el tipo penal del artículo 269 G ("Suplantación de sitios Web para capturar datos personales", que afectarían al acceso, almacenamiento y transmisión de datos).

Como tipos agravados de estos tipos básicos sería la actual conducta delictiva del artículo 269 D (Daño informático), porque afecta a los datos personales, a un sistema informático, red informática o programa de computación (software).

El actual tipo delictivo básico de obstaculización ilegítima de sistema informático o red de telecomunicaciones, afecta en esta última parte a una red de telecomunicaciones. La Ley

---

(26) RIASCOS GOMEZ, Libardo O. ***Los datos personales informatizados en el derecho foráneo y colombiano*. Análisis de las fases del Proceso Informático.** En: http://akane.udenar.edu.co/derechopublico.

1341 de 2009 o Estatuto de las TIC en Colombia, sostiene en el artículo 10º que *la provisión de redes y servicios de telecomunicaciones,… es un servicio público bajo la titularidad del Estado, (que) se habilita de manera general, y causará una contraprest*ación periódica a favor del Fondo de las tecnologías de la información y las comunicaciones" del Ministerio de Tecnologías de la Información y las comunicaciones.

El término telecomunicación [27] cubre todas las formas de comunicación a distancia, incluyendo radio, telegrafía, televisión, telefonía, transmisión de datos e interconexión de ordenadores a nivel de enlace. El estatuto de las TIC excluye de su regulación lo atinente a la televisión y al servicio postal, las cuales deberán seguir rigiéndose por las leyes especiales para cada medio de comunicación.

La obstaculización ilegítima en las redes de comunicación se diferencia de la interceptación en las comunicaciones en que la primera hace referencia a cualquier forma de interferencia en la emisión o recepción de la información a través de uno cualquiera de los medios de telecomunicación; en cambio, la interceptación es la acción precisa de captación de las comunicaciones entre el emisor y el receptor para conocer el contenido de las comunicaciones, a través de medios de grabación de sonidos, voz o imagen o de copia, xerocopia o transcripción del contenido de comunicaciones escritas mecánicas, electromecánicas o informáticas.

4.2.7. Sub Tipo de Intrusión: *"El Superzapping*". Según el tratadista Reyna Alfaro [28], una de las modalidades de impedir u obstaculizar el uso o acceso a sistemas, datos o redes de telecomunicaciones es a través del uso de "llaves maestras" o programas computacionales no autorizados, lo cual se conoce como *Superzapping.* Esta especie de intrusismo informático afecta al acceso de la información bien impidiendo ingresar por los canales establecidos en el programa, sistema o red de telecomunicación, o bien poniendo trabas tecnológicas para el correcto uso o utilización del sistema, base o red de redes de información.

4.2.8. Reforma: *Ut supra* hemos planteado que la conducta comentada y prevista en el Artículo 269 B del C.P., perfectamente puede insertarse en un tipo general de *violación de los datos, los sistemas informáticos o redes de información,* en el cual ocuparían el lugar del inciso 3º, por afectar a la tercera fase del proceso de tratamiento de datos luego de la recolección y almacenamiento; tratamiento propiamente dicho y registro y, finalmente la consulta y transmisión de datos.

El proyecto de ley presentado a la Cámara de Representantes para reformar el Título VII Bis del C.P., referido a "la Información y los datos" personales, no propone reformas específicas al texto previsto en el artículo 269 B, pese a que el término normativo del tipo "sin estar facultado para ello", refiriéndose a la persona que impide u obstaculiza el funcionamiento o el acceso "normal" a un sistema informático, o a los datos informáticos allí contenidos, o a una red de telecomunicaciones, resulta innecesario, por estar previsto dicho elemento de antijuridicidad en la parte general del Código, pues si actúa facultado para impedir u obstaculizar el funcionamiento o acceso a los sistemas o bases informáticas devendría la atipicidad de la conducta y no estaríamos ante un hecho delictivo.

Es cuestionable el término utilizado por el legislador del 2009 al referirse al "*acceso normal*",

---

(27) La **telecomunicación** (del prefijo griego *tele*, "distancia" o "lejos", "comunicación a distancia") es una técnica consistente en transmitir un mensaje desde un punto a otro, normalmente con el atributo típico adicional de ser bidireccional. En: http://es.wikipedia.org/wiki/Telecomunicaci%C3%B3n. Enciclopedia WIKIPEDIA.

(28) Citado por CASTRO OSPINA,J. Ob., ut supra cit. 5

por cuanto el acceso es una actividad computacional que sólo se viabiliza si se tiene una clase, contraseña, filtro de ingreso o cualquiera otra medida de seguridad que permita o impida el acceso a secas, pues informáticamente no existe acceso anormales sino accede o no accede a un sistema o base informática. Esa función no es calificable de normal o anormal, sino de viabilización o no del acceso. Aún los hackers al ingresar a un sistema o base informática lo hace una vez desencriptan unos signos alfanuméricos, reconocen una clave o encuentra una contraseña con programas computacionales rastreadores, fisgones o reveladores de claves o "destripadores" (Por lo de "Jack" el destripador), pero al fin y al cabo el acceso se produce.

4.3. DELITO DE INTERCEPTACION DE DATOS INFORMÁTICOS

4.3.1. Fuente Normativa: Artículo 269 C. Concordante con los Artículos 192-196 C.P. del 2000.

Son aplicables a este conducta algunas de las normas jurídicas mencionadas en el delito de "violación ilícita de la comunicaciones", prevista en el artículo 192 del C.P., por tratarse de fenómenos tecnológicos parecidos y hasta actividades humanas sobre esos fenómenos homologables, si se tiene en cuenta que la interceptación no se hace de medios de comunicación tradicionales sino de aquellos permeados por las nuevas tecnologías TIC, con la diferencia concreta que el artículo 269 C, se refiere a la interceptación de datos informáticos que incluye datos personales inmersos o no en sistemas informáticos, bases de datos o redes de telecomunicaciones por medios informáticos, electrónicos o telemáticos. Estos son:

(i) La Ley 1341 de 2009, sobre la conceptualización de los nuevos medios de la información y la comunicación o TIC, régimen jurídico de la telefonía fija y móvil e infracciones contravencionales que afectan al derecho de la intimidad, el honor y demás libertades y derechos constitucionales cuando existen actuaciones ilícitas en las comunicaciones; (ii) El Decreto 075 de 2006, *Por medio del cual se definen las obligaciones que le asisten a los operadores de servicios de telecomunicaciones en procura de optimizar la labor de investigación de los delitos por parte de las autoridades competentes".* La Fiscalía General de la Nación es el organismo del Estado encargado de la coordinación con los organismos con funciones de Policía Judicial, del manejo de las actividades y procesos relacionados con la interceptación de los servicios de telecomunicaciones; (iii) El Artículo 235 C.P.P., reformado por la Ley 1142 de 2007, reglamenta el procedimiento de interceptación de las comunicaciones telefónicas y similares, realizadas por la Fiscalía mediante la grabación magnetofónica o similares y el artículo 237 Id, sobre audiencia de control de legalidad posterior sobre la interceptación, por parte del juez de control de garantías.

4.3.2. El tipo penal. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) y setenta y dos (72) meses.

4.3.3. Sujetos de la conducta: El sujeto activo de la conducta es una persona sin calificación alguna y puede ser particular o servidor del Estado. Este último tendrá mayor punibilidad por su connotación de vinculación con el Estado, los privilegios y derechos que como funcionario tiene y su mayor insidiosidad frente a la conducta penal (artículo 269 H-2 del C.P.). También se puede decir que puede ser una persona particular o una jurídica, esta última a través de su representante legal o miembro de aquella.

No solo el Estado, sino las Agencias de Información financiera o comercial, los operadores y las fuentes que administran, manejan o coordinan bases, ficheros o registros de datos, entre otros pueden ser sujetos pasivos de la conducta.

4.3.4. La confidencialidad, la integridad y la disponibilidad de la información. Con esta conducta punible se afectan los tres estadios de la información: su confidencialidad, la integridad y la disponibilidad que son precisamente el núcleo esencial del bien jurídico tutelado de la Información y los datos personales.

Sobre la confidencialidad, el secreto o sigilo de la información; así como de la disponibilidad de la información, caracterizada por la restricción de la libre circulación de la misma (artículo 4-c [29], Ley 1266 de 2008), han quedado explicados en las anteriores conductas ilícitas, por eso en este aparte nos referiremos a la integridad de la información.

La integridad de la información está íntimamente relacionada con el principio de veracidad o calidad de los registros o datos, que consiste en *que la información contenida en los bancos de datos debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el registro y divulgación de los datos parciales, incompletos, fraccionados o que induzca a error* (artículo 4-a, Ley 1266 de 2008).

Se afecta la integridad de la información entonces, cuando se impide u obstaculiza su funcionamiento o el acceso a la misma. Esa conducta la ejecutan los conocidos Hackers o intrusos. "*Las modalidades más conocidas son las siguientes: Las bombas lógicas (Logic bombs), que se producen en un sistema informático y se activan con un comando especial (fecha, números, etc.), para destruir o dañar datos contenidos en un ordenador; ejemplo,… los conocidos virus Sycam y Dragón Rojo…*

4.3.5 Conceptualizaciones: La figura penal trae varios términos técnicos que merecen ser explicados. Algunos ya han sido explicados ut supra, tales como Interceptación de datos, sistema informático y datos informáticos; pero otros como el espectro electromagnético y origen o fuente de información se aclara así:

Espectro electromagnético: "Es un bien público inenajenable e imprescriptible sujeto a la gestión y control del Estado. Se garantiza la igualdad de oportunidades en el acceso a su uso en los términos de ley" (art.75 CN).

Ley 1341 de 2009, sobre "principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones —TIC—, crea la Agencia Nacional de Espectro como una dependencia del Ministerio de tecnologías de la información y comunicación. La ANET, se encarga de permitir, inspeccionar, vigilar y controlar el uso del espectro electromagnético y sancionar a quienes lo vulneren o desconozcan. En efecto, constituye infracción hace un uso negativo del espectro es una infracción (art.64-13).

Técnicamente, también podemos entender el espectro electromagnético de la siguiente forma: la *"Franja de espacio alrededor de la tierra a través de la cuales se desplazan las ondas*

---

(29) La administración de datos personales se sujeta a los límites que se derivan de la naturaleza de los datos, de las disposiciones de la presente ley y de los principios de la administración de datos personales especialmente de los principios de temporalidad y la finalidad del banco de datos.
Los datos personales, salvo la información pública, no podrán ser accedidos por internet o por otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o los usuarios autorizados conforme a la presente ley.

radioeléctricas que portan diversos mensajes sonoros o visuales" y son reproducidas, transmitidas o transportadas por medios de comunicación tradicionales o por medios pertenecientes a las nuevas tecnologías de la información y la comunicación TIC, es decir, por medios informáticos, electrónicos o telemáticos.

Según el artículo 4-a, Ley 1266 de 2008, fuente de información, es *la persona, entidad u organización que recibe o conoce datos personales de los titulares de la información, en virtud de una relación comercial o de servicio o de cualquier otra índole y que, en razón de autorización legal o del titular, suministra esos datos a un operador de información, el que a su vez los entregará al usuario final. Si la fuente entrega la información directamente a los usuarios y no, a través de un operador, aquella tendrá la doble condición de fuente y operador y asumirá los deberes y responsabilidades de ambos. La fuente de la información responde por la calidad de los datos suministrados al operador, la cual en cuanto tiene acceso y suministra información personal de terceros, se ajusta al cumplimiento de los deberes y responsabilidades previstas para garantizar la protección de los derechos del titular de los datos.*

Con estos conceptos se aclara que la interceptación de datos se puede dar en su origen (fuentes de información), en su destino (operadores de la información), o en el interior de la misma (operador que administra y pone en conocimiento la información a los diferentes usuarios autorizados para ello).

4.3.6. Verbo Rector: Interceptar. Todo lo mencionado al comentar el entendimiento del verbo rector interceptar medios de comunicación y telecomunicación en el delito de violación ilícita de las comunicaciones prevista en el artículo 288 del C.P., de 1980, así como en el punible del mismo nombre en el artículo 192 del C.P., del 2000, son válidos en este aparte en toda su plenitud. La diferencia en la conducta punible del artículo 269 C, como se comentó antes era en que la interceptación de los medios tecnológicos de información y comunicación, TIC, a través de la informática, electrónica y telemática se da exclusivamente sobre datos personales visuales, auditivos, de voz o imágenes. Muy a pesar de ello, ya en esa oportunidad dijimos que dicha interceptación de medios de comunicación perfectamente podían interpretarse que se extendían a los medios TIC, aún antes de que existiera esta forma delictiva específica del artículo 269 C.

4.3.7. Tipo básico de control visual y/o auditivo clandestino. En el derecho español la conducta de interceptación de datos informáticos hace parte de un tipo básico de control visual y/o auditivo clandestino y de las conductas de control ilícito de señales de comunicación. Esto quiere decir que la conducta prevista en el artículo 269 C, hace más referencia a la "*incriminación de conductas de interceptación, grabación o reproducción ilícita de otros medios de comunicación, como por ejemplo las comunicaciones por telefax o por correspondencia informática"* [30], o también de los medios de comunicación que envían o recepcionan datos personales a través de canales informáticos, electrónicos o telemáticos.

La tratadista Castro Ospina [31], ubica al "pinchado de líneas (*Wiretapping*)" como una conducta delictiva que afecta la confidencialidad de la información y quizá junto a otras conductas como la introducción de datos falsos (*data diddling*), la fuga de datos (data leakage), uso de llaves maestras (*superzapping*), son los *"ataques más graves del derecho de*

---

(30) MORALES PRATS, Fermín. ***Comentarios a la parte especial del Derecho penal. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio***. Ed. Aranzadi, Pamplona (España), 1997, p. 303.

(31) CASTRO OSPINA, J. Ob., ut supra cit. 5

la información, como bien colectivo y que ponen en peligro derechos individuales…" como la intimidad, el honor, la imagen, el buen nombre, el habeas data y el propio derecho a la información.

4.3.8. Reforma: La propuesta de reforma al delito de interceptación de datos informáticos es significativa no sólo por el mejoramiento en la redacción del tipo penal básico, sino por ampliar la cobertura del tipo con la utilización de nuevos verbos rectores y el aumento de la punibilidad acorde con la mayor insidiosidad de la figura delictiva y las acciones del agente del delito.

La nueva conducta delictiva que se propone es la siguiente: "***Interceptación, control o sustracción de datos informáticos.*** *El que, sin la existencia de orden judicial previa intercepte, controle o sustraiga datos informáticos en su origen, destino, transmisión o en un sistema informático o telemático, o las emisiones electromagnéticas provenientes de un sistema informático o telemático que las transporte, incurrirá en pena de prisión cuarenta y ocho (48) a noventa y seis (96) meses y en multa de cien (100) a mil (1000) Salarios mínimos legales mensuales vigentes"*

Desde el mismo intitulado de la conducta penal cambia, pues ya no sólo es punible la mera interceptación, sino el control o sustracción de los datos, es decir, el apoderamiento de los datos informáticos, siempre que se haga sin orden judicial previa. Esta conducta ilícita afecta a la confidencialidad, integridad y disponibilidad de la información.

En el derecho español al redactar el tipo penal básico del *"descubrimiento y revelación de secretos"* del artículo 197 del C.P. Español de 1995, en la primera parte del inciso primero decidieron tipificar el delito de apoderamiento de documentos, papeles, cartas, mensajes de correo electrónico "o cualesquiera otros documentos" o de efectos personales, dirigido al desvelar la intimidad de las personas; y en la segunda parte del primer inciso, tipificaron la interceptación de telecomunicaciones o utilización de artificios técnicos de escucha, transmisión, grabación o reproducción de sonido o de la imagen, o de cualquier otra señal de comunicación, con el objeto de desvelar la intimidad de las personas contenidas en datos personales escritos, auditivos, visuales o telemáticos (imagen, voz y audio). En uno y otro caso, se establece una actividad delictiva de control auditivo y/o visual clandestino, tras el apoderamiento físico de los datos o por la captación, grabación o filmación de aquellos datos.

Sin embargo, el tratadista ibérico *Morales Prats* [32] sostiene, que debía darse un trato punitivo distinto al simple apoderamiento de los datos personales para desvelar la intimidad de las personas de aquella en la cual se utilizan "*sofisticados aparatos de control auditivo o visual clandestino* (grabación, escucha o interceptación de comunicaciones habladas o filmación-captación de imágenes)*; éstos últimos proporcionan un control certero y sistemático, más penetrante que pasa inadvertido para la víctima*". Esto significaría una mayor sanción punitiva para el control auditivo o visual clandestino que para el mero apoderamiento físico de los datos, "documentos o efectos personales".

Ahora bien, en el derecho colombiano tras la proposición de la reforma al artículo 269 C, se coloca en el mismo plano punitivo tanto la interceptación de datos, como el apoderamiento de datos informáticos, aunque la acción punitiva sea alternativa al utilizar los verbos interceptar, controlar o sustraer, hubiese sido más conveniente que se excluyera la sustracción, por ser un término equivoco que puede significar apoderamiento o hurto de datos que desnaturaliza la interceptación y control de datos, pues se entiende que quien intercepta datos de alguna

---

(32) MORALES PRATS, Fermín. ***Ob., ut supra cit.***, p. 303.

manera los está aprehendiendo visualmente (es decir en pantalla, si se trata de datos informáticos interceptados en un equipo de computador propio o de terceros), documentalmente (si se imprimen los datos a través de equipos idóneos para esa tarea), auditivamente (si se escuchan directamente en la interceptación, o una vez se han grabado mediante los aparatos específicos para esta tarea) o visual auditivamente (si se observan y escuchan en un aparato de video o video-filmadora, o en una presentación de video en un aparato de computador, esté o no en línea o red de redes de comunicación).

La Convención de Budapest de 2001, recomienda a los países miembros de la Unión Europea, UE, tipificar la interceptación ilícita (deliberada o ilegítima), por medios técnicos de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático a otro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos. Se recomienda además, que el tipo delictivo que se erija en estas condiciones, se sostenga que se haga con intención delictiva o "*en relación con un sistema informático conectado a otro sistema informático".*

Si bien en el derecho colombiano se siguieron las pautas generales al elevar a tipo penal las conductas de interceptación de señales de comunicación y emisiones electromagnéticas o radioeléctricas, no se cumplió con la estructuración de la interceptación ilícita como tal, sin adiciones del control y menos aún de la sustracción, pues por lo general los datos informáticos bienes intangibles que pueden tangibilizarse en la medida que se saquen de la red, el sistema informático o el banco de datos, mediante aparatos idóneos (impresoras, escáner, cámaras de video o fotográficas, etc.). Si bien no sobra tanto el término "control" en el tipo penal colombiano, ya hemos dicho antes que la interceptación presupone que al aprehenderse los datos de alguna forma (visual, audiovisual o auditiva) se ejerce un control sobre los mismos con fines ilícitos, por ello la sola interceptación es suficiente para indicar la insidiosidad de la conducta y los fines que se persigue, más cuando en el artículo 269 H, sobre circunstancias de agravación punitiva se dice que los tipos penales básicos perteneciente al Capítulo VII bis del C.P., y entre ellos el del artículo 269 C (que se ha propuesto reformar el Congreso de la República, mediante la figura que comentamos), se comente "obteniendo provecho para sí o para un tercero" (numeral 5º), o con fines terroristas o generando riesgo para la seguridad o defensa nacional (numeral 6º), o utilizando como instrumento a un tercero de buena fe (numeral 7º). Este "tercero" se conoce eufemísticamente, como "mulas informáticas" las cuales actuando de buena fe y sin conocimiento del ilícito en el que participan no son punibles.

Es acertada la reforma del tipo penal del artículo 269 C, en lo referido a la utilización de los elementos normativos de "transmisión o en un sistema informático o telemático" para referirse a la forma como puede interceptarse un dato informático, en el origen, destino o transmisión (que reemplaza al término "en el interior" de un sistema informático, que producía ajenidad con el fenómeno o tratamiento de datos). Igual la adición del término "telemático" para indicar que un sistema informático, también lo puede ser "telemático" (audio, sonido e imagen), tanto para transmitir datos informáticos como para ser contenedor de datos auditivos, sonoros o de imagen. Sin embargo, recuérdese que un sistema informático es omnicompresivo de datos, hechos o circunstancias contenidos en un tratamiento o procesamiento de datos e interconectados entre sí, por dispositivos computacionales de hardware y software, y como es obvio, los datos pueden ser informáticos, electrónicos o telemáticos.

4.4. DELITO DE DAÑO INFORMATICO

4.4.1. Fuente Normativa: Artículo 269 D sobre el Daño Informático. Concordante con éste los artículos 265 sobre el delito de daño, el 272-3 sobre violación de los mecanismos de

protección de los derechos patrimoniales de autor; y el artículo 58-17 sobre causales de mayor punibilidad, cuando se realiza una conducta penal con medios informáticos, electrónicos o telemáticos. Además, el Convenio de Budapest de 2001.

El Artículo 265 del actual C.P., estructura el delito de *daño en bien ajeno*, así: "*El que destruya, inutilice, haga desaparecer o de cualquier otro modo dañe bien ajeno, mueble o inmueble incurrirá en prisión ....*"

Si se resarciere el daño ocasionado al ofendido o perjudicado antes de proferirse sentencia de primera o única instancia, habrá lugar al proferimiento de resolución inhibitoria, preclusión de la investigación o cesación de procedimiento.

Se dice con alguna razón que sobraba erigir como delito el daño informático, porque no era más que compatibilizar el artículo 265 con el artículo 58-17 de la parte general del C.P., pues perfectamente de la aplicación sistemática resultaba el daño informático con una dosimetría de punición mayor a la que plantea el artículo 269 D.

Más aún, el actual artículo 272 del C.P*,* al tipificar la *Violación a los mecanismos de protección de los derechos patrimoniales de autor y otras defraudaciones*", estructura penalmente una especie de daño informático ocasionado a los "componentes lógicos de un programa de computación (software) o sistema informático o tratamiento de datos que hace parte teleológica del delito de daños informático. En efecto, quien: "*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***" –cursivas y negrillas nuestras--.

El Convenio de Budapest de 2001, cuando solicita a los Estados Miembros erigir en conducta penal, la "***interferencia en los datos"*** (diferente a "la interferencia en el sistema" que nuestro país se reguló como obstaculización en el sistema informático o red de telecomunicaciones", artículo 269 B), consiste en la "*comisión deliberada e ilegítima de actos que dañen, borren, deterioren o supriman datos informáticos*" y se recomienda además que se estipule no solo los daños ocasionados, sino "graves daños" en los datos.

En tal virtud, dicho convenio propone como más ajustado a la realidad del tratamiento o procesamiento de datos, la "interferencia en los datos", puesto que aquí caben todas las acciones contra los datos, sean o no sinónimos de daños: borrar, deteriorar o suprimir datos informáticos.

El Código Penal Colombiano en el artículo 269 D., utiliza un mayor número de acciones, verbos rectores para ejemplificar el delito de daño informático, así: destruir, borrar, deteriorar, alterar, suprimir y dañar.

4.4.2. El tipo penal. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48)

4.4.3. Sujetos de la conducta delictiva: Por la utilización de la partícula "El que", significa que puede ser agente del delito cualquier persona particular o servidor del Estado, solo que en éste último caso, por las connotaciones, derechos, deberes y privilegios del servidor del

Estado en la rama, organismo, dependencia o destino público donde labore será mayor la sanción punitiva, según lo determina el artículo 269 H., del Título VII Bis del Código Penal.

Los sujetos pasivos del ilícito serán el Estado, pero también las personas naturales o jurídicas que administren, dirijan o coordinen bases o bancos de datos, sistemas informáticos o registros informáticos dentro o fuera de la red de redes de comunicación.

4.4.4. La integridad y disponibilidad de la información. La conducta delictiva por los verbos utilizados para su estructuración afecta la información a la integridad y la disponibilidad de la información. Vale decir, afecta la esencia misma de la información, el contenido de la misma, su validez (contrario al dato erróneo), certeza (contrario al dato falso), eficacia (contrario al dato desactualizado), calidad y completud (contraria al fraccionamiento, al dato incompleto) de la información.

Respecto de la disponibilidad de la información, la conducta evita que la información y los datos se puedan transmitir, comunicar o circular en forma incompleta, errónea, confusa, inválida, ineficaz o desactualizada o sea falsa, pues todas estas formas de disponibilidad de la información constituyen una interferencia en los datos o "daño informático" en términos del derecho penal colombiano.

4.4.5. Conceptualizaciones. El tipo penal de daño informático, contiene varios términos técnicos propios de la informática jurídica [33] y aplicables al derecho penal. Unos de esos términos ya los hemos comentado ut supra, tales como datos informáticos y sistema informático. Otros resultan propios del artículo 269 D., son: "Sistema de tratamiento de información" y "componentes lógicos". Uno y otros términos no han sido abordados por la Ley 1266 de 2008, ni por los proyectos anteriores a la Ley 1273 de 2009, que en su artículo 1º relacionaban algunos términos técnico-informáticos utilizados por la ley en la descripción de cada tipo penal.

La Directiva Europea 96/45/CE, relativa al procedimiento informático de los datos personales y en defensa de derechos como la intimidad, relaciona lo que debemos entender por *Sistema de Tratamiento de información*, así: "Cualquier operación o conjunto de operaciones, efectuadas o no mediante procedim*iento automatizados, y aplicables a los datos personales, como la recogida, registro, organización, conservación, elaboración, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquiera otra que facilite el acceso a los mismos, el cotejo o interconexión, así como su bloqueo, supresión o destrucción*". En otros términos, se consideran las diferentes fases o etapas por las cuales deben pasar los datos personales o informáticos para su debido tratamiento dentro y fuera de una red de redes, o en un sistema informático o base o banco de datos desde la recolección, almacenamiento, registro, comunicación, circulación transferencia de datos ("flujo internacional de datos", se conoce en normas internas europeas, como en la Ley 15 de 1999 o ley de tratamiento "automatizado" de datos personales en España).

El término "*o sus partes*" relatado a continuación del sistema de tratamiento de información es ajeno a una explicación informática, pues sí el sistema es un procedimiento informático de tratamiento de datos, es lógico que se pueda afectar a una parte o todo el procedimiento, pero eso en informática poco importa pues los procedimientos son concatenaciones casi inseparables y si falta alguna no funciona la estructura total, salvo el caso que el tratamiento lo realicen diferentes personas.

---

(33) RIASCOS GOMEZ, Libardo O. ***La Constitución de 1991 y la informática Jurídica.*** Ed. UNED, Universidad de Nariño, Pasto, 1997, p. 10 ss.

Los “componentes lógicos” son los programas de computador o Software. Este término en español o en inglés debió utilizarse por ser menos equivoco que aquél.

Todo tratamiento informatizado de datos incluye dos componentes inseparables como son el Hardware y el Software, es decir, la parte física y lógica del computador, por eso el daño informático al que se refiere la norma en el presente delito, es el daño logicial que se produce a los datos informáticos, aunque existen algunos programas de computador, conocidos como “Bombas Lógicas” y Variados Virus, que no solo afectan a la parte lógica de los programas y a los datos en ellos contenidos, sino que existen verdaderos daños materiales al disco duro y unidades periféricas informáticas, porque los inutilizan o hacen que no sea posible volverlos a utilizar, solo por excepción pueden ser recuperables mediante mantenimiento técnico.

Pensamos que si el daño ocasionado al Hardware o parte material del computador no está cubierto con esta conducta delictiva del artículo 269 D, bien podría aplicarse el artículo 265 del C.P., del delito de daño aplicable a todo bien, incluidos los informáticos.

4.4.6. Verbos rectores alternativos: Los verbos rectores son: Dañar, Destruir, borrar, deteriorar, alterar o suprimir.

Hemos dicho que el Tipo básico de daño Informático, se configura con una serie de verbos consecutivos o alternativos que en el diccionario de la lengua castellana resultan ser sinónimos algunos y por tanto no necesariamente deberían incluirse por estar supuestos en la sinonimia. V.gr. Dañar, destruir, deteriorar. Inclusive según dicho diccionario sinónimo de dañar es inutilizar, estropear, arruinar, menoscabar, entre otros. Sin embargo, los tipos penales deberían en aras a hacer un honor al idioma no colocar todos los términos sinónimos si con el principal “*dañar*” se subentienden los demás.

Se asimilan a daño no siéndolo en estricto rigor, pero sí comprensible en la informática jurídica, los verbos borrar, alterar o suprimir. Estos términos son entendibles en informática, porque borrar o eliminar un dato informático, significa sacarlo de la memoria de un programa, pero con programas de computador avanzados se puede recuperar (“desborradores” o recuperadores de los datos borrados en la memoria de un PC., e incluso de los un correos electrónicos borrados de un buzón personal o institucional. En todo caso, son recuperables y por tanto el daño podría ser temporal. Es tal tecnología informática que existen programas que recuperan información de discos duros “formateados” o “inicializados”, que se entiende que el borrado de datos es casi definitivo).

La alteración (sinónimo de destruir, descomponer) de un dato informático, significaría el cambio de contenido, previa ingreso mediante el acceso al mismo, levantando la medida de seguridad o clave que éste tenga.

Suprimir es sinónimo de borrar o eliminar un dato o información general o específica.

4.4.7. Revisión: En el delito de daño en el derecho penal español se ubica bajo el bien jurídico protegido de los delitos contra el Patrimonio y contra el orden económico social, artículos 263 a 267. En el Artículo 264-2 C.P., como tipo penal agravado presenta el delito de daño informático “*al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informático*”, que resulta más coherente pues al fin y al cabo el delito de daño realizados sobre bienes lógicos (software) o bienes físicos (hardware) utilizados en informática en esencia no cambia con el daño que se puede infligir a cualquier otro bien, salvo como parece ser la intención del tipo de daño informático en nuestro derecho, que se justifica el tipo penal específico de daño informático porque va dirigido a los datos informáticos, a la

esencia misma de la información que por su puesto esté contenida en un soporte lógico (CD, Disquete, memoria USB, memoria de un disco duro o flexible, etc.), pues de lo contrario no se justificaría su estructuración. Sin embargo, es tan débil la cuerda de distinción entre producir daño a la parte logicial de un programa y los datos informáticos allí contenidos, porque es inescindible una de los otros, que el daño ocasionado a uno deviene indefectiblemente al otro y por tanto, la estructuración del delito de daño informático (sin decirlo así expresamente el C.P., Español, tan solo redactarlo como se ha transcrito) es perfectamente aplicable al daño logicial y físico computacional.

En el derecho penal español el tratadista *Quintero Olivares* [34], explica porque el legislador reglamentó *los daños sobre programas o documentos electrónicos ajenos,* por fuera de los específicos bienes jurídicos que protegían otros derechos. Manifiesta: *Esta expresa tipificación obedece al temor del legislador a que el mencionado objeto (datos, programas electrónicos ajenos obtenidos en redes o sistemas informáticos), especial por su naturaleza y por su ubicación (informática) no tuviera una completa protección penal, ya que, si el Código cuenta con una expresa mención a estos objetos, frente a sustracciones o apoderamientos en los delitos relativos al mercado y los consumidores (artículo 278-1 CP), así como la que pueda corresponder en cuanto propiedad intelectual (artículo 270 CP), también era precisa la regulación de su destrucción o inutilización, que a su vez, se puede cometer tanto por una actuación como a través de las vías del propio sistema informático*.

4.4.8. Reforma. El proyecto de ley reformatoria del Título VII Bis del C.P., colombiano, propone la eliminación de los siguientes elementos normativos del tipo: "Sin estar facultado para ello", por cuanto resulta presupuesto en la antijuridicidad del tipo penal, tal como se expone en la parte general del C.P. En efecto, sí está facultado para realizar las acciones descritas en el tipo deviene la atipicidad del delito. Igualmente si quien realiza esas labores o acciones (verbos rectores del tipo), tiene el consentimiento del titular de los datos informáticos, también se desnaturaliza la figura delictiva.

También se propone la eliminación de demasiados verbos rectores y dejarlos en dañar, destruir o "alterar de modo sustancial" datos informáticos, sistemas informáticos…"**.** Esto es acorde con lo que decíamos anteriormente. Pese a ello, sigue sobrando el término "alterar de modo sustancial" datos informativos y otros medios informáticos o telemáticos, pues si se cambia o suprimen, borrar o dañan la destrucción del dato o el sistema siempre es significativa aunque parezca que es insignificante materialmente, pero desde el punto de vista informático lo es.

4.5. DELITO DE USO DE SOFTWARE MALICIOSO

4.5.1. Fuente Normativa: Artículo 269E del C.P., adicionado por la Ley 1273 de 2009

4.5.2. El tipo penal. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios legales mensuales vigentes.

4.5.3. Sujetos de la conducta penal: El agente de la conducta puede ser cualquier persona sin calificación alguna, es decir, un particular como un servidor de Estado. En iguales

---

(34) OLIVARES QUINTERO, Gonzalo. ***Comentarios a la parte especial del Derecho penal. Delitos contra el Patrimonio y el Orden Económico Social***. Ed. Aranzadi, Pamplona (España), 1997, p. 560.

condiciones y observaciones que para los anteriores tipos delictivos el servidor del Estado responde más severamente por sus actuaciones en vista de que tener la calidad de servidores del Estado es causal de agravación punitiva, según el artículo 269 H-2, del C.P. Iguales razonamientos se da en el caso de los sujetos pasivos que puede ser el Estado, o las personas naturales o jurídicas, públicas o privadas, según fueren administradores, directores de Agencias de Información comercial u operadores de bases o bancos de datos.

4.5.4. La integridad y la disponibilidad de la información.

La conducta delictiva del uso de software malicioso, tan criticado desde el nomen iuris por los propios legisladores colombianos [35], afecta la integridad o esencia misma de la información, como la transmisión, comunicación o circulación de la información por las vías y canales informáticos o telemáticos.

4.5.5. Conceptualizaciones

La conducta contiene dos términos técnico-informáticos que en realidad son uno. Estos son: "software malicioso" y "programas de computación". En efecto, software según traducción al castellano generalizada es programa de computador o parte lógica de un programa computacional. De ahí que sobra repetir software y programa de computación. La diferencia entre los dos es la utilización equívoco y innecesario en el tipo penal de "*malicioso*", todo por la traducción literal que se da a "*Malware*" sinónimo de "*Bad ware*".

En efecto, *"Malware"*, proviene del inglés "*malicius*" o malicioso (sinónimo de pícaro, bellaco, astuto, ladino, sagaz, etc.). Características todas que se predican de una persona humana, no de un objeto inanimado como sería un programa de computador. Quizá esa sea la crítica válida al sobrenombre de "Software" de "malicioso", porque no concuerda el objeto (programa de computador) con el sobrenombre propio de las personas (malicioso); pero lo correcto sería entender que se quiere significar con "Software malicioso" y darle una significación no literal al término.

Software [36] en principio se entiende como (soporte o equipamiento lógico), *es la suma total de programas de computo, procedimientos, reglas, documentación, manuales y datos asocia-*

---

(35) Decía el Senador Parmenio Cuellar Bastidas, al proponer el archivo del proyecto 281 de 2008, relativo a la modificación del C.P., al crear un nuevo bien jurídico denominado de la "Información y de los datos", que una de entre otras debilidades de dicho proyecto era "que estas conductas… ni siquiera tienen una equivalencia en nuestra lengua materna (castellano) y no resulta de recibo hacer depender las consecuencias, de la traducción de las palabras inglesas; mucho menos pueden hacerse tipos que describan conductas que solo tienen sentido en su denominación en inglés. Eso es cierto, pero hoy por hoy el fenómeno informático, electrónico y telemático es universal, como universales son los términos ingleses en la informática general y en particular en la jurídica que obligan a todos los profesionales del derecho a actualizarse cada día en estos menesteres pues la universalización también ya llegó al derecho permeado por las nuevas tecnologías de la información o comunicación TIC y ya no es extraño encontrar en textos jurídicos citas textuales, contextuales y mucho más términos específicos en otro idioma al materno y eso es una forma explícita de la universalización del derecho que ha entrado ahora a leyes, códigos, estatutos de diferentes ramas del derecho. En: ***Informe de ponencia para primer debate al proyecto 281 de 2008***. Senador Parmenio Cuellar . Bogotá, Mayo 14 de 2008, p. 5.

(36) Esta conceptualización se estipulaba en el artículo 1º del proyecto de ley previo a la Ley 1273 de 2009. Además, **Troyanos,** programa malicioso o dañino disfrazado de software inofensivo, que puede llegar a tomar control de la computadora, con miras a provocar el daño para el que fue creado. **Virus.** Programa o código de programación transmitido como un adjunto de mail o dispositivo que permite su réplica, copiándose o iniciando su copia o reproducción en otro programa de ordenador o equipo de cómputo. **Gusano.** Programa o código de programación transmitido como un conjunto de mail que se replica copiándose o iniciando su copia en otro programa, sector de booteo de una computadora, o documento, pero que no requiere de un portador para poder replicarse.

dos que forman parte de las operaciones de un sistema de cómputo. Esta conceptualización ya se tenía en Colombia desde la expedición del Decreto 1360 de 1989, de 23 de Junio.

Malicioso o "*Bad ware*", es aquel software que tiene como objetivo infiltrarse en una computadora o dañarla sin el consentimiento de su propietario y/o usuario. Existen diferentes tipos de malware: Virus informáticos, troyanos, gusanos, programas de *Spyware/adware* e incluso los bots, "*Crash programs*" y cáncer routines, así como cualquier otra técnica igual o similar que se desarrolle en el futuro.

El Spyware que es una especie de "*Software malicioso*" (que mejor sería decir uso o utilización ilícitos de programas de computador). El "*Spyware*" son programas de computador que se instalan sin el conocimiento del usuario para recolectar y enviar información de manera no legítima. A su vez, una subespecie de Spyware, es el *Bulo u Hoax* [37] con los cuales mediante una forma engañosa y atrayente vía correo electrónico o invitación a utilizar un programa por el cual puede reenviar dicha información falsa o engañosa con diferentes fines alarmistas pero no para sacar provecho alguno.

Si eso es así bastaba en el derecho colombiano con elevar a rango delictivo las conductas que realizaran las personas que hace *uso ilícito o indebido de los programas de computador*, diferentes a los que ya estaban legislados para la propiedad intelectual, industrial o empresarial. Eso si se quiere abarcar todos los verbos rectores que trae el actual artículo 269 E, en el delito de uso de software malicioso, pues de lo contrario, el estricto uso ilícito de programas lo que provoca es una especie de daño específico en los programas de computador o en la parte logicial de los ordenadores y para ello, no era más que erigir como tipo penal agravado del delito de daño informático, en un inciso 2º del artículo 269 D, el uso ilícito de programas de computador que tiendan a dañar datos personales, sistemas informáticos o sistemas de tratamiento informático en bases o bancos de datos, con una pena mayor a la estipulada en dicho artículo.

4.5.6. Verbos alternativos: El tipo penal de "uso de software malicioso", utiliza una serie de verbos rectores que en nuestro sentir desbordar el verdadero intitulado de la conducta o simplemente no es significativa de todas las implicaciones que le suministran los elementos normativos del tipo. En efecto, los verbos alternativos utilizados para la construcción de la figura delictiva son: *Producir, traficar, adquirir, distribuir, vender, enviar, introducir, extraer.* Curiosamente no utiliza el verbo usar que le da el título al ilícito penal, lo que hace más sospechosa la estructuración del tipo y la ajenidad de la redacción del tipo con el título del delito que lo contiene. Más aún se pensaría que tal como está redactado debería estar mejor

---

(37) Un **bulo** u Hoax es la noticia falsa es un intento de hacer creer a un grupo de personas que algo falso es real. En el idioma español el término se popularizó principalmente al referirse a engaños masivos por medios electrónicos especialmente internet./ Las personas que crean bulos tienen diversas motivaciones dentro de las que se encuentran el satisfacer su amor propio, la intención de hacer una broma para avergonzar o señalar a alguien o la pretensión de provocar un cambio social haciendo que la gente se sienta prevenida frente a algo o alguien; también suele ser característico dentro de los autores de bulo el querer mofarse y hacer evidente la credulidad de las personas y de los medios de comunicación. / ***El bulo informático.*** Es un mensaje de correo electrónico con contenido falso o engañoso y atrayente. Normalmente es distribuido en cadena por sus sucesivos receptores debido a su contenido impactante que parece provenir de una fuente seria y fiable o porque el mismo mensaje pide ser reenviado. /Las personas que crean **bulo** suelen tener alguno de los siguientes objetivos: (i) Captar direcciones de correo (para mandar spam, virus, mensajes con phishing o más bulo a gran escala); (ii) Intentar engañar al destinatario para que revele su contraseña o acepte un archivo de malware; (iii) Confundir a la opinión pública de la sociedad. Básicamente, los bulos se dividen en las siguientes categorías: 1. Alertas sobre virus incurables, 2. Mensajes de temática religiosa, 3. Cadenas de solidaridad, 4. Cadenas de la suerte, 5. Métodos para hacerse millonario, 6. Regalos de grandes compañías, 7. Leyendas urbanas, y 8. Otras cadenas. En: http://es.wikipedia.org/wiki/Bulo.

ubicado entre los delitos que protegen la propiedad intelectual y previstos en el artículo 52 de la Ley 44 de 1993, pues se trata de proteger no los datos personales que es la esencia del Título VII bis, sino evitar la producción, tráfico, distribución o comercialización de programas de computador que tengan "efectos dañinos", que fácilmente se puede deducir que son programas no autorizados, ilegales, piratas, etc., y que además producen daños logiciales en sistemas informáticos, datos informáticos o tratamiento de datos o bases datos.

Una reforma oportuna a los delitos contra la propiedad intelectual que abarque los nuevos fenómenos de la informática y las tecnologías TIC, debería aprovecharse para que los tipos penales que atentan contra la propiedad intelectual en el derecho colombiano pasaran a integrar un capítulo específico dentro del Título correspondiente a los delitos contra la propiedad para integrar mejor la protección al bien jurídico protegido de los diferentes tipos de propiedad (tales como la general y la industrial que sí están integradas al C.P. vigente. Esta integración la tiene el C.P., Español de 1995 y se protege con demasiado ahínco la propiedad intelectual (artículos 270 a 272).

Por lo tanto, es muy cuestionable la redacción de este tipo penal, los fines contrarios al título del tipo penal que persigue y sobre todo sí la figura penal está bien ubicada entre los delitos que protegen la información y los datos.

Probablemente algunas de estos cuestionamientos se pueden explicar, además de las razones jurídicas anteriormente sostenidas, en que los hechos o circunstancias que surgen de atentados contra la información día a día y devenidos de las nuevas tecnologías de la información y la comunicación TIC, por abarcarlos todos y reprimirlos con una conducta típica, antijurídica y culpable, se redactan atendiendo más al fenómeno informático y sus efectos dañinos en la práctica diaria con sistemas informáticos o sistemas de tratamiento informático o bases de datos (todas las especies de "Software" mal llamado "malicioso") que a la estructuración de un tipo penal con conceptos jurídicos claros, precisos pero basados en el hecho tecnológico y no al revés.

4.5.7. Reforma: La propuesta de reforma al artículo 269 E, elimina el término normativo constitutivo del ilícito "sin estar facultado para ello" y lo cambia a "con fines ilícitos" para referirse al cúmulo de verbos rectores que estructuran el delito. Este cambio, no parece ser significativo, porque el primer término como hemos dicho en otras figuras delictivas era innecesario, pues en la primera parte del Código Penal al referirse a la antijuridicidad de los tipos penales se prevé que las conductas se realizan sin facultades para ello, sin autorización, sin permiso, etc., pues de lo contrario las conductas dejan de ser típicas.

El término "con fines ilícitos", utilizado para estructurar el tipo, si bien mejora la redacción y el entendimiento del delito, la verdad es que la ajenidad sigue produciéndose entre el nomen iuris del delito y la redacción total del tipo, aunque se hay incluido ahora el verbo "*usar*" que no estaba previsto en el artículo 269 E. y se haya eliminado los términos ("del territorio nacional" y "otros programas de computación de efectos dañinos") y verbos innecesarios (introducir o extraer) y se haya adicionado equívocamente ("o intrusivo" y al final del tipo "siempre que la conducta no constituya delito sancionado con pena mayor").

En efecto, la propuesta del nuevo artículo es la siguiente: "Uso de software malicioso. El que, con fines ilícitos, produzca, trafique, adquiera, distribuya, venda, use o envíe software malicioso o intrusivo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de cien (100) a mil (1000) salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena mayor".

Al introducir el término *"intrusivo*" luego de "*software malicioso o*", el tipo cambio de ser un subtipo agravado del delito de daño informático, tal como lo habíamos propuesto *ut supra,* para convertirse en un subtipo agravado del delito de acceso abusivo a un sistema informático, previsto en el artículo 269 A. Y esto último es precisamente lo que los traicionó el subconsciente a los legisladores reformadores del tipo del artículo 269 E., al colocar in fine del tipo, la frase "*siempre que la conducta no constituya delito sancionado con pena mayor*".

Paradójicamente, la pena imponible para el delito 269 A y la propuesta de reforma del artículo 269 E., son exactamente iguales y por lo tanto, la frase in fine del tipo reformador será letra muerta.

4.6. DELITO DE VIOLACION DE LOS DATOS PERSONALES

4.6.1. Fuente Normativa: Artículo 269F del C.P., adicionado por la Ley 1273 de 2009.

4.6.2. El tipo penal. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y multa de 100 a 1000 S.M.M.V.

4.6.3. Sujetos de la conducta penal: El agente de la conducta puede ser cualquier persona sin calificación alguna, es decir, un particular como un servidor de Estado. En iguales condiciones y observaciones que para los anteriores tipos delictivos el servidor del Estado responde más severamente por sus actuaciones en vista de que tener la calidad de servidores del Estado es causal de agravación punitiva, según el artículo 269 H-2, del C.P

Iguales razonamientos se da en el caso de los sujetos pasivos que puede ser el Estado, o las personas natural o jurídico, público o privado, según fueren administradores, directores de Agencias de Información comercial u operadores de bases o bancos de datos, en los términos de la Ley 1266 de 2008 o Ley de Habeas Data.

4.6.4. La Confidencialidad, integridad y la disponibilidad de la información. Esta conducta penal afecta a los tres aspectos objeto de protección del Título VII Bis, por cuanto se prevé el acceso, almacenamiento, transmisión, interceptación y divulgación de los datos personales, bases de datos y sistemas informáticos y de tratamiento de datos. En estas circunstancias, la confidencialidad, integridad y disponibilidad de la información se ve afectada por cualquiera de estas acciones que realice el agente en forma sucesiva o alternativa. Este tipo penal, como antes se dijo es el que debería iniciar el presente Título VII Bis de los delitos contra la información y los datos porque abarca todo el procedimiento o tratamiento de datos personales que son una especie del género datos informáticos y por cuanto prevé varios verbos rectores que afectan a las diferentes etapas o fases de dicho procedimiento (desde el recolección, almacenamiento, registro, transmisión o circulación de datos). A partir de esta figura delictiva se debieron organizar los demás tipos como quedó expuesto anteriormente.

4.6.5. Conceptualizaciones. El tipo penal de violación de datos personales previsto en el artículo 269 F, prevé varios términos normativos estructurales del tipo de carácter técnico que ya hemos aclarado anteriormente (v.gr. datos personales), pero también prevé unos nuevos, tales como códigos personales, ficheros, archivos, "bases de datos o medios semejantes".

Para asumir dichos conceptos debemos consultar la norma extrapenal prevista en la Ley 1266 de 2008, la cual en su artículo 3, literales *e*, al *h*, nos define:

Datos Personales: *Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de la ley. Datos pueden ser públicos, semiprivados o privados*.

Dato público. *Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas;*

Dato semiprivado. *Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV de la presente ley*. Estos "servicios" en el título y a lo largo de toda la ley no se especifican por lo que debemos entender que son en principio los estipulados en la Ley 142 de 1994, es decir, los servicios públicos domiciliarios (Electricidad, agua, telefonía y gas).

Dato privado. *Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular*.

Los términos ficheros (del francés "ficheirs") y bases de datos, son sinónimos, pues son utilizados en el derecho español indistintamente en sus leyes protectoras de datos personales o de tratamiento "automatizado" de datos; en cambio, en el derecho francés por supuesto es utilizado sólo el término ficheirs.

En consecuencia, ***fichero o bases de datos (database),*** significa Cualquier conjunto de informaciones que sea objeto de un tratamiento o procedimiento informatizado, así geográficamente estén dispersos pero interconectados.

El término "o medios semejantes", se entenderían además de los que en el futuro se invente para almacenar, transmitir o circular datos entre diferentes puntos geográficos y por diversos medios tecnológicos informáticos, electrónicos o telemáticos, los que actualmente se conocen. V.gr. los ***sistemas informáticos***, entendidos como todo dispositivo aislado o conjunto de conectores interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa de ordenador o computador.

Los ***Códigos personales*** (o medidas de seguridad de acceso a la información instaladas por el titular de los datos para guardar la confidencialidad o secreto de la información que le concierne) son contraseñas, claves o password utilizados por las personas para acceder a un programa o sistema informático sin que otras personas puedan hacerlo por él, ya que estos son secretos, únicos y de sirven de autenticación del ingreso para su titular. Estas contraseñas suelen ser fáciles de adivinar porque utilizan nombres de personas más queridas, de mascotas, de objetos preciados, de personajes de cine, novela o de ciencia ficción, dioses de la mitología griega, de animales exóticos, números telefónicos conocidos, direcciones residenciales, fechas de nacimiento o muerte de seres queridos o cualquier otra fecha relevante, nombres de ciudades o países donde se ha vivido y hasta palabras en idiomas extranjeros que se conozca o no; o en fin, situaciones, hechos o circunstancias que rodean la vida personal del titular de los datos o las que por defecto vienen de fábrica en programas comercializados v.gr. 1234, 0000, 9999 o 5555. Las Contraseñas mediano o difíciles de averiguar, son aquellas que no están asociadas a ninguna de las anteriores situaciones,

hechos o circunstancias y utilizan signos alfanuméricos y pasan de seis letras con sus dígitos numéricos adicionales. Sin embargo, estas últimas son las de más difícil recuerdo para el usuario y por regla general se anotan en alguna parte (libretas, libros, agendas, archivos informáticos o documentos electrónicos, puestos en la red de redes, etc.) y terminan siendo más vulnerables que las primeras, si se encuentran con por Hackers (White and Black), sobre todo las que se ponen irresponsablemente en archivos o documentos electrónicos expuestos a que un pirata cibernético los halle más fácilmente que si se hubiese escondido en un vetusto libro empolvado olvidado en algún rincón de la casa, pues en este punto al menos sigue predicándose que: "My Home is my castle".

Mitnick [38], en su libro *El Arte de la Intrusión* dedica un capítulo eufemísticamente titulado: "Anécdotas breves", en las cuales comenta ocho novelescos casos en los cuales las contraseñas en programas de computador son tan irrisorias que cualquier principiante podría adivinarlas, p.e., en un programa de computador que maneja una máquina de refrescos, pudo ser manipulado por un hacker, porque utilizaron como clave, el título de la marca de la competencia. Sí el propietario de la máquina de refrescos es Coca-Cola, ¿Cuál es la clave del programa utilizado por éstos?. Increíble: Pepsi.

Una **contraseña** o **clave** (en inglés ***password***) es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña normalmente debe mantenerse en secreto ante aquellos a quien no se le permite el acceso. Aquellos que desean acceder a la información se les solicitan una clave; si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso [39].

4.6.6. Verbos alternativos. La conducta punitiva de violación de datos personales prevista en el artículo 269 F., utiliza varios verbos rectores consecutivos y alternativos para estructurar el tipo. Estos son: Obtener, sustraer, ofrecer, compilar, vender, intercambiar, enviar, comprar, interceptar, divulgar, modificar o emplear. Esta amplia gama de acciones humanas inmersas en un solo tipo si bien abarcan diferentes posibilidades en las que puede quedar incurso una persona que actúa frente a los "*códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes*", no es menos cierto que pueden presentarse equívocos en la acertada utilización de los mismos que podrían llevar a indebidas incriminaciones, como mínimo. Otro aspecto negativo de este excesivo número de verbos resulta de utilizar acciones propias de los dispositivos informáticos, electrónicos o telemáticos como "compilar", "enviar", "intercambiar", "interceptar", "divulgar" con actividades humanas como "comprar", "sustraer", "ofrecer", "obtener" y "emplear", o que pueden realizar unos y otras, como: "enviar", "comprar o vender", porque habrá momentos en que una u otra acción se solapen a través de los dispositivos informáticos y se desnaturalice el tipo penal.

Para evitar estas excesivas listas de verbos rectores en los tipos penales referidos a la informática es mejor seguir las pautas de los Estados que vienen estructurándolos y poniendo en funcionamiento no solo textual sino en la práctica diaria por que tienen varios casos que han judicializado y sentenciado y porque además tienen estadísticas de lo sucedido y aprende del error y acierto de normas jurídicas comunitarias como internas en cada Estado miembro de la UE.

---

(38) MITNICK, Kevin. ***El arte de la intrusión. Cómo ser un hacker o evitarlos.*** Ob.ut supra cit., p. 337. Cuenta además las anécdotas de la pérdida de sueldo; ven a Hollywood, pequeño mago; Merma del ejército Iraquí durante la "tormenta del desierto"; El Cheque regalo del mil millones de dólares; el Robot del Póker; El joven cazador de pedófilos; y "ni siquiera tienes que ser un hacker".

(39) En: http://es.wikipedia.org/wiki/Contrase%C3%B1a

El Convenio de Budapest de 2001, después de analizar las varias propuestas para tipificar delitos que protejan penalmente los datos personales, pues se entiende que existe una normatividad iuscivilista y iusadministrativa de *prima ratio* para protegerlos preventivamente, fue proponerles a los Estados Miembros, erigir como delito la "*comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos*", en lo que llama "interferencia en los datos" (artículo 4º), para distinguirla de *la interferencia en el sistema*, consistente en "*la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático, mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración y supresión de datos informáticos"* (artículo 5º)

4.6.7. Reforma. La propuesta de reforma del delito de violación de datos personales no propone cambio alguno. Sin embargo, creemos que al igual que en las anteriores conductas delictivas es conveniente excluir de la redacción los siguientes elementos normativos de estructuración del tipo penal: "*sin estar facultado para ello*" y adicionar el término omnicomprensivo pero menos criticable que el anterior: "con fines ilícitos". También debería eliminarse los términos: "*con provecho propio o de un tercero*", puesto que según el artículo 269H, relativo a las circunstancias de agravación punitiva para todos los tipos penales básicos del Titulo VII bis le son aplicables y por supuesto, la causal quinta de dicho artículo es realizar la conducta "*obteniendo provecho para sí o para un tercero*" que al ser aplicada al ilícito del artículo 269 F, se entendería que el legislador de 2009 ya había regulado un tipo penal básico como si fuera agravado desde su origen y eso significa cuando menos, una falta de técnica legislativa y una incoherencia jurídico-criminológica que para los demás tipos penales deja un estructura básica con la posibilidad de ser agravada sí se dan las causales del artículo 269 H, en dos etapas comisivas del ilícito y no en una sola para el caso comentado.

De otro lado téngase en cuenta que la violación de los datos personales contenidos en archivos, bases de datos o sistemas informáticos podrían involucrar aquellos datos que en legislaciones europeas (El Convenio de Europa de 1980, artículo 7º y la Ley 15 de 1999 o Ley de tratamiento "automatizado" de datos personales en España, por ejemplo), prohíben o restringe al máximo hacerlo puesto que se afecta el llamado "núcleo duro de la privacidad, como son los datos personales sobre el origen racial o étnico, las creencias, la salud, la vida sexual o afiliación política, ideológica o laboral.

Algunas de las razones de esta prohibición o máxima restricción a la recolección, almacenamiento, registro o transmisión o flujo internacional de datos personales son proteger los derechos de la persona, tales como la intimidad personal y familia, el honor y la buena imagen que en todas las Constituciones Europeas se han elevado a rango constitucional y por tanto, de potenciada protección. Además porque, al afectar el "núcleo duro de la privacidad", las legislaciones internas deberán reduplican las medidas de seguridad, sí deciden no prohibir definitivamente la recolección o cualquier otro tratamiento informatizado identificada o identificable de datos, sino permitir someter a tratamiento informatizado de datos dichos datos sensibles de la persona, con el pleno de garantías sustantivas o procesales para proteger integralmente los derechos y libertades fundamentales de la persona. En ambos casos, la protección efectiva del Estado y de los mismos particulares será evidente y altamente reforzada en el plano jurídico de prima y de última ratio [40].

En nuestro país en el ámbito de prima ratio no existe una protección integral, aunque sí mínima de los datos personales pertenecientes al núcleo duro de la privacidad, pues la legislación interna no ha producido normas iuscivilistas o iusadministrativistas dirigidas a la protección del derecho a la intimidad, el honor, la imagen, el buen nombre, aunque sí sobre el

---

(40) RIASCOS GOMEZ, Libardo O. ***El derecho a la intimidad, la visión iusinformática y los delitos relativos a los datos personales.*** *Tesis Doctoral, Universidad de Lleida (España), 1999, p. 324.*

derecho a la información (Ley 57 de 1985, "Estatuto de la Información"; Ley 190 de 1995, "Estatuto anticorrupción"; Ley 527 de 1999, "Documentos e Información electrónica"; Ley 594 de 2000, "Estatuto de Archivos públicos y privados"; y, Ley 962 de 2004, "Estatuto antitrámites") y el derecho fundamental del habeas data (con una demora imperdonable en el contexto latinoamericano, el legislador colombiano expidió --tras las reiteradas invitaciones de la Corte Constitucional para hacerlo en sus fallos de tutela sobre el habeas data--, una ley sectorial e incompleta, conocida en la doctrina como "Ley del Habeas Data financiero o comercial", Ley 1266 de 2008 [41]).

En el ámbito de última ratio, el legislador colombiano ha proferido normas contravencionales contenidas en el Código Nacional de Policía de 1970 y 1971, para proteger el derecho a la intimidad domiciliaria, así como la "vida íntima" y "vida privada" de las personas en los artículos 46 a 49 y 52, al elevar a contravenciones especiales los atentados contra la inviolabilidad de domicilio personal y familiar, como el del sitio de trabajo, así como la inviolabilidad de la vida íntima o privada de las personas en el seno de su hogar o sitio de trabajo, ya sea que se atente con aparatos tradicionales o subrepticios de grabación o filmación de sonidos, imágenes o voces. Tal como quedó reseñado y comentado anteriormente.

En el Código Penal de 1980 dentro de las causales de agravación punitiva no se vislumbraba causal alguna que se refiera a los aspectos integrantes del núcleo duro de la privacidad en el artículo 66 que posibilitaran agravar la sanción si se cometía delito alguno que incorpore aspectos o datos personales sobre el origen racial o étnico, las creencias, la salud, la vida sexual o afiliación política, ideológica o laboral.

En la parte general del Código Penal del 2000 el artículo 58 hizo eco de las legislaciones universales al respecto y por fin estipuló unas causales de mayor punibilidad del tipo penal básico sí "*la ejecución de la conducta punible esté inspirada en móviles de intolerancia y discriminación referidos a la raza, la etnia, la ideología, la religión, o las creencias, sexo u orientación sexual, o alguna enfermedad o minusvalía de la víctima*".

En consecuencia, cualquier conducta punible que se cometa inspirados en los anteriores "móviles de intolerancia y discriminación", tal como denomina a los datos sensibles o integrantes del núcleo duro de la privacidad o intimidad nuestro C.P., vigente, la sanción tendrá una mayor punibilidad, máxime si la comisión se realiza con medios informáticos, electrónicos y telemáticos (artículo 58, numerales 3º y 17º, respectivamente).

En el actual artículo 269 F, --pues las propuestas de reforma a éste tipo penal básico ya no lo hizo— como circunstancia de agravación punitiva se podrá aplicar las previsiones del artículo 58, numerales 3º y 17º, por ser perfectamente viables e idóneas para crear un tipo penal complementario de agravación punitiva que requiere la existencia del tipo básico y la concurrencia de las circunstancias de mayor punibilidad mentadas.

4.7. DELITO DE SUPLANTACION DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES

4.7.1. Fuente Normativa: Artículo 269G, adicionado al C.P. del 2000 por la Ley 1273 de 2009.

---

(41) RIASCOS GOMEZ, Libardo O. ***El habeas Data: una visión constitucional, legal y en proyectos de ley estatutaria.*** *En* http://akane.udenar.edu.co/derechopublico

4.7.2. El tipo penal. El que, con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 SMMV, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

4.7.3. Sujetos de la conducta penal: El agente de la conducta puede ser cualquier persona sin calificación alguna, es decir, un particular como un servidor de Estado. En iguales condiciones y observaciones que para los anteriores tipos delictivos el servidor del Estado responde más severamente por sus actuaciones en vista de que tener la calidad de servidores del Estado es causal de agravación punitiva, según el artículo 269 H-2, del C.P

Iguales razonamientos se da en el caso de los sujetos pasivos que puede ser el Estado, o las personas natural o jurídico, público o privado, según fueren administradores, directores de Agencias de Información comercial u operadores de bases o bancos de datos, en los términos de la Ley 1266 de 2008 o Ley de Habeas Data.

4.7.4. La Confidencialidad, integridad y la disponibilidad de la información. La conducta sui generis de “suplantación de sitios de web para capturar datos personales” afecta los tres aspectos objeto de protección del C.P., en el título VII bis, puesto abarca todo el ciclo informático desde la recolección, almacenamiento, registro, transmisión o flujo de datos personales, y por lo tanto, se pretende prevenir el acceso, la revelación, la comercialización y la transmisión de los datos que le conciernen a la persona.

La conducta es sui generis, porque trasplanta el fenómeno tecnológico tal y como sucede en la vida diaria para convertirlo en conducta punible y no las acciones humanas que vayan encaminadas a proteger el bien jurídico protegido en éste título: La Información y los datos personales, o más aún, los derechos fundamentales de la intimidad, el buen nombre, la imagen y el habeas Data. De esta forma se procede en el Inciso 1º y 2º.

Cierto es que el fenómeno tecnológico posibilitado mediante medios informáticos, electrónicos y telemáticos, se conoce ampliamente no solo la suplantación de sitios web con miras a diversas actividades ilícitas, sino además el solapamiento de sitios web, el superzapping en los sistemas informáticos, etc., todas violando medidas de seguridad de acceso, claves, contraseñas o códigos personales y conocidas genéricamente como formas de *intrusismo informático en red de redes o internet* que persiguen finalidades ilícitas.

Si para “suplantar” un sitio de Web y capturar datos, hay que previamente acceder o ingresar al sitio violando las medidas de seguridad tecnológica, bien estructurado legislativamente éste delito de intrusión informática para capturar datos sería en un inciso del anterior delito violación de datos personales, pues al fin y al cabo el contenido que cambia en el presente delito es la forma e insidiosidad de ingresar a los sitios de Web con el propósito de capturar datos personales, aunque este fin ilícito solo esté previsto en el intitulado del delito y en el inciso 2º , cuando avanza a capturar datos personales o financieros. Por ello, resulta innecesario la tipificación de esta forma delictual si para ello sólo se traspola el fenómeno

tecnológico a la conducta punitiva que persigue proteger la confidencialidad, integridad y disponibilidad de la información con una serie de verbos rectores que se compadecen con el intitulado del delito, como precisaremos *ut infra.*

Cierto es también, que como lo indica el inciso 2º del artículo 269 G, también se convierte en actividad punible con igual sanción a la del tipo básico de "suplantación de sitios de web", aquel que "modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza". Es decir, aquella persona que acceda a un sistema informático, base de datos o sistema de tratamiento de datos personales o financieros modificando "los nombres de dominio [42]" o direcciones electrónicas asignadas autorizada y debidamente en forma tecnológica a las personas naturales o jurídicas para poder navegar por la Internet e identificarse con nombres o abreviaturas, por el ejemplo, los dominios de los gobiernos estatales con ***.gov***, los de las universidades e instituciones de educación con ***.edu;*** los de las empresas, industrias con ***.com;*** las instituciones y entidades militares, con ***.mil;*** las organizaciones***,*** organismos de tipo, objetivos y actividades diferentes a las anteriores, con .***org***, **etc.**

En este segundo inciso, el legislador del 2009 excedió su capacidad de trasplantar el fenómeno tecnológica a la tipificación de conductas delictivas porque especificó que la modificación de los nombres de dominio estarían dirigidos a ilicitudes en *"bancos o a otro sitio personal o de confianza*" (que más fácil y omnicomprensivo debió decir a datos financieros o personales), y aunque no indica que sea con fines y provechos ilícitos, se entiende que el mero *vouyerismo informático* que comentábamos anteriormente en el delito de acceso abusivo a un sistema informático (artículo 269 A), no es lo que mueve al intruso informático o "*White hacker*". Entonces, si quien modifica el nombre de dominio hace ingresar equívocamente a una persona a un sitio de web de un banco u otro personal o de confianza, incurriría en la figura penal del inciso 2º del artículo 269 G., pero si además consigue una "transferencia de activos en perjuicio de un tercero" incurrirá en el delito de transferencia no consentida de activos, prevista en el artículo 269 J del C.P., y esto significaría que es innecesario haber tipificado el fenómeno tecnológico simplemente de acceso de los "nombres de dominios" sólo con el propósito explícito de modificarlo, sin saber para qué hacerlo. Menos mal, que este tipo penal mutilado remite en blanco, al decir: "siempre que la conducta no constituya delito sancionado con pena más grave". En efecto, esa frase hace que debamos remitirnos al artículo 269 J, que tiene una punibilidad mayor y complementa el tipo penal incompleto del artículo 269 G, inciso 2º.

El inciso 3º del artículo 269 G., prevé un tipo penal agravado de los anteriores tipos penales básico (Inciso 1º) y el mutilado (Inciso 2º), cuando para la consumación del ilícito se requiere que "*el agente (haya) reclutado víctimas en la cadena del delito*", es decir, una especie de "mula informática", que es aquel "tercero que obra de buena fe" y es utilizado como "instrumento" en la consumación del delito. Esta actividad ya está prevista como causal de agravación punitiva en el artículo 269 H, numeral 7º, entendiendo que este tercero si actúa en esas condiciones estaría exento de responsabilidad penal, de lo contrario deberá evaluarse su grado de participación en el ilícito.

---

(42) Un **dominio de Internet** es una etiqueta de identificación asociada a un grupo de dispositivos o equipos conectados a la red internet. El propósito principal de los nombres de dominio en internet y del sistema de nombres de dominio (DNS), es traducir las direcciones IP de cada modo activo en la red, a términos memorizables y fáciles de encontrar. Esta abstracción hace posible que cualquier servicio (de red) pueda moverse de un lugar geográfico a otro en la red internet, aún cuando el cambio implique que tendrá una dirección IP diferente. Sin la ayuda del sistema de nombres de dominio, los usuarios de internet tendrían que acceder a cada servicio web utilizando la dirección IP del nodo (Ej. Sería necesario utilizar http://74.125.45.100 en vez de http://google.com). En: http://es.wikipedia.org/wiki/Dominio_de_Internet

Pese a lo dicho, el legislador penal de 2009, en el aparte transcrito del artículo 269 G., no habla de "tercero" sino de "víctima" calificando a priori que todos los que se encuentren en la calidad de "reclutados" en la consumación del tipo penal automáticamente serán víctimas y eso en el mundo de la informática jurídica es como mínimo no cierto, pues en el mundo de las nuevas tecnologías TIC, muchas veces se confunde la víctima con el victimario. Baste leer el libro del Arte del Intruso de Kevin Mitnick, uno de los principales hacker enjuiciado y condenado en los Estados unidos para comprender lo dicho.

4.7.5. Conceptualizaciones. La sui generis conducta delictiva de suplantación de sitios de Web para capturar datos personales con propósito ilícito genérico, contiene una serie de términos técnico-informáticos que en determinado momento soslayas la redacción del tipo penal en tal grado que no parece estar leyendo un conducta penal sino un reporte de cómo se puede realizar, negociar o enviar una página de web y qué efectos tiene hacerlo.

Los términos utilizados en informática jurídica son: (i) "Sitios de Web", "páginas electrónicas", o "sitio personal o de confianza"; (ii) "enlaces o ventanas emergentes"; (iii) "nombres de dominio"; y, (iv) "IP".

Para entender el concepto de páginas WWW o Web, debemos hablar del llamado hipertexto (HTML: HyperText Markup Language), al cual no referimos en otra obra jurídica [43].

El Hipertexto es el hijo primogénito y más genuino de la información y comunicación electrónica y telemática. Con el nacimiento del Hipertexto no sólo se han establecido nuevas formas tecnológicas TIC en unión con la informática, sino una estructura de comunicación electrónica *sui géneris:* interactiva, global, sin límites geográficos y de trasmisión (emisión/recepción) de información de todo tipo, por universidades, instituciones, Centros u Organismos privados y públicos en formatos, con funciones, características y velocidades electrónicas, siempre y cuando se cuente con un software y hardware idóneos.

El Hipertexto, como otros medios de comunicación electrónica, está basado en los términos anglosajones apocopados de *Hyper Text Markup Language* (HTML)[44], que gramaticalmente significa: Lenguaje textual gradualmente incrementado, aunque se ha difundido universalmente como hipertexto que subsume las características de gradualidad, vinculación e incremento, entendibles en nuestra lengua castellana con el prefijo "*hiper*". Igualmente se ha considerado el HTML, como el formato utilizado por las páginas de texto creadas exclusivamente para ser colocadas en una red de redes de información por el proveedor respectivo.

El Hipertexto tiene una forma (interna y externa) y un fondo. La forma externa del hipertexto hace relación a la construcción textual con formatos de página WEB, es decir, con metodología World Wide Web (WWW); en tanto que la forma interna hace referencia a la parte técnica y configuración del sotfware apto para elaborar dichas páginas. Aquí, por obvias razones, nos referiremos a la forma externa, pues la interna es objeto de la informática estructural. En efecto, para que un ordenador muestre toda la información en pantalla, y luego un usuario pueda emplearla informáticamente como cualquier información digital: almacenar (storage), editar (edit), transferir o simplemente consultarla en el monitor del ordenador debe crearse por parte de los proveedores de información (universidades, centros, etc.), las denominadas páginas WEB dentro

---

(43) RIASCOS GOMEZ, Libardo O. ***El derecho a la intimidad…Ob., ut supra cit****, p. 453.*

(44) Vid. El HTML. "Se trata de un lenguaje de descripción de páginas que reproduce el contenido y aspecto de la página WWW de tal forma que los diferentes programas de acceso (como Internet Explorer) pueden representarla con la forma que desee". TORBEN RUDOLPH, Mark. ***Todo sobre el internet explorer*** *4.* Ed. Marcombo, Barcelona,1998, p.128.

de un espacio de un servidor de internet denominado "*Webspace*" . La publicación de páginas en el mundo virtual del WWW, conocida como *Webpublishing ,* siguiendo los pasos que determinan los diferentes software expertos, son: a) Disponer de un espacio necesario en internet (Webspace), previamente determinado por un proveedor de servicios de comunicación electrónica; b) Con el software idóneo se crea las páginas WEB de información según las pautas, principios, características y funciones del proveedor de la información respectiva. Las páginas se escriben como si fuese con cualquier programa de ordenador que procesa texto común y corriente, pero con algunas diferencias técnico-estructurales, que no son del caso comentarlas ahora. Las páginas creadas y diseñadas de conformidad con los fines y objetivos del informador, se almacenan en memoria central y auxiliar del ordenador; y c) Las páginas creadas y almacenadas conforman lo que se denomina el *homepage*, o sea, las páginas matrices de la información que ofrece el proveedor correspondiente. El proveedor de la información la enviará luego mediante su servidor de comunicación electrónica a la red de red de información (v.gr. Internet), para que comience a navegar en las autopistas de la información y sean utilizadas por los usuarios o internautas previos el acceso a la dirección y sitio de la red prefijado por el proveedor de la información.

Otras formas externa del hipertexto, lo constituyen las posibilidades que tienen las páginas WEB, para incorporar imágenes fijas y en movimiento (vídeo), ilustraciones o gráficos (dibujos multifacéticos) e incluso sonidos (voz, música o cualquiera otra fuente que genere sonido). Esta forma que constituye a la vez una de las principales características de las páginas WEB, conforman un ambiente especial de comunicación electrónica que une las ventajas y características de la multimedia **[45]** y las del hipertexto. Algunos iusinformáticos han llamado a este *sui* géneris y especial matrimonio tecnológico TIC y la informática como *Hipermultimedia* o simplemente *Hipermedia, según Marshall Brain* **[46]**. Quizá la principal virtud del hipertexto sea la alta capacidad para incorporar en sus páginas información textual, visual y de sonido, pues como nunca antes la información se presenta ante el usuario tranquila tranquilamente sentado frente a su ordenador situado en una aula de la universidad, en su casa, en su empresa; en fin, en cualquier lugar donde haya un computador conectado a una red de información capaz de emitir y recepcionar señales de comunicación electrónica. La información producida y recepcionada por el usuario o internauta constituye el espejo de la realidad (realidad virtual), en tiempo real, concomitante o diferido, según factor *in témpore* en el que es recibida. Todo ello sin moverse físicamente del sitio de trasmisión o consulta de la información, pues el navegante electrónico es un caminante sin desplazamiento en el espacio geográfico.

Otro aspecto de forma externo del hipertexto, lo constituye la interactividad de los escritos, páginas WEB, y sobre todo, documentos electrónicos construidos con el lenguaje HTML. La interactividad posibilita al usuario enlazar documentos electrónicamente con cualquiera otro que guarde relación con aquél, no sólo como lo hace el documento tradicional escrito con las referencias bibliográficas, citas de pié de página o remisiones internas o externas en un libro, sino y además, en forma dinámica, cuando puede consultar concomitantemente con el documento en pantalla las referencias bibliográficas, citas o remisiones en todo su contexto, y a la vez, las que aquél documento consultado refiere, y así sucesivamente en forma escalonada o gradual, hasta donde el interés del usuario-consultante se halle satisfecho (y muchas veces más

---

(45) Normalmente se entiende por multimedia, a la utilización de los nuevos medios de comunicación basados en productos digitales o servicios que integran texto, gráficos, audio, película o vídeo, fotografía o animación, combinados con herramientas de software, los cuales permiten a los usuarios actuar de forma recíproca con estos. La multimedia puede presentarse en forma de productos de CD-ROM, en programas de ordenador ofrecidas en los kioscos, en servicios *on line* en los sitios de la red de redes de información mundial (WWW), y en las tecnologías de realidad virtuales. Vid. JARVLEPP, Harry. B.A., LL.B., M.B.A. *INFORMATION TECHNOLOGY AND NEW MEDIA LAW*. En: ***KnowledgeBase. An information Technology Law Bulletin***- Fall 1997. En: WWW.Umontreal.edu.ca

(46) Citado por KATSH, *Ethain.* ***Rigths, camera, action****. O*b. ut supra cit. En: WWW.Umontreal.edu.ca

allá) e ir a las mismas fuentes de producción de los documentos consultados por el enlace, sin importar el sitio geográfico donde se hallen, el tiempo horario real en el que se hace; el ambiente locativo en el que se halle (biblioteca privada o pública, siempre que no haya restricción al acceso electrónico); todo ello, con sólo identificar una dirección, ruta, camino electrónico (http:// WWW.,--http:**H**ypertext **T**ransfer **P**rotocol, es decir, la trasmisión de documentos electrónicos por hipertexto-- v.gr. Http:www.elcano.com. Buscador para páginas en español), o también conocido como *sitio en el WEB* o URL (**U**niform **R**essource **L**ocator) [47].

Los vínculos [48] o enlaces electrónicos de un escrito o documento ibídem, pueden ser tantos como desee hacerlos el creador del documento, el usuario o consultante o el almacenador de la información. Los vínculos en una página WEB de hipertexto no sólo une documentos textuales, sino que también permite insertar imágenes fijas o de vídeo (formatos BMP), gráficos en formatos GIF (***G**rafic **I**nterchange **F**ile*) o JPG (***J**oint **P**hotography **G**roup*) que potencian la presentación de documentos electrónicos e igualmente una amplia variedad de sonidos en diversos formatos (WAV, MIC, etc.). Esa potencialidad de vinculación de multimedia y texto, se denomina *hipervículo* [49].

Una **dirección IP** [50] es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (*Internet Protocol*), que corresponde al nivel de red del protocolo TCP/IP. Esta dirección puede cambiar cada vez que se conecta; y a esta forma de asignación de dirección IP se denomina una *dirección IP dinámica* (normalmente se abrevia como *IP dinámica*).

Los sitios de Internet que por su naturaleza necesitan estar permanentemente conectados, generalmente tienen una *dirección IP fija* (se aplica la misma reducción por *IP fija* o *IP estática*), es decir, no cambia con el tiempo. Los servidores de correo, DNS, FTP públicos, y servidores de páginas web necesariamente deben contar con una dirección IP fija o estática, ya que de esta forma se permite su localización en la red.

A través de Internet, los ordenadores se conectan entre sí mediante sus respectivas direcciones IP. Sin embargo, a los seres humanos nos es más cómodo utilizar otra notación más fácil de recordar y utilizar, como los nombres de dominio; la traducción entre unos y otros se resuelve mediante los servidores de nombres de dominio DNS.

El ***Pop up***: Denota un elemento (ventana) emergente que se utiliza generalmente dentro de terminología Web, y finalmente, el ***Link:*** es un enlace o acoplamiento informático.

4.7.6. Verbos Rectores utilizados por el tipo penal básico, el mutilado y el agravado.

El tipo penal básico utiliza varios verbos para estructurar la conducta tales como diseñar, desarrollar, vender, ejecutar, programar, enviar (páginas electrónicas, enlaces o ventanas emergentes). Todas estas acciones están precedidas de los términos normativos del tipo: “con objeto ilícito” y “sin estar facultado para ello”. Los dos términos como hemos sostenido en otras figuras penales de éste Titulo VII bis, son innecesarios por estar previstos en el parte general del Código al estructurar la antijuridicidad de la conducta, pues se entiende que si no se realizaran con fines ilícitos la conducta sería atípica.

---

(47) TORBEN RUDOLPH, Mark. *TODO SOBRE*... Ob. ut supra cit., pág. 248
(48) Ibídem, pág. 264.
(49) KATSH, *Ethain. RIGTHS, CAMERA,:... O*b. ut supra cit. En: WWW.UMONTREAL.EDU.CA
(50) **En: http://es.wikipedia.org/wiki/Direcci%C3%B3n_IP**

Quizá el legislador penal del 2009 estimó conveniente anteponer el término “objeto ilícito” para no caer en contradicción evidente de punir actividades lícitas como diseñar, desarrollar o programar una página de internet o “vender” datos personales “sin el consentimiento de su titular”, por ejemplo. La ilicitud de la conducta debió afincarse en la falta o vicio del consentimiento del titular de los datos, el cual es vulnerado por el agente de la conducta para realizar cualquier actuación ilícita con los sitios, páginas o portales de web o electrónicas, incluido el acceso, el almacenamiento, trasmisión o circulación de datos personales o peor aún sensibles o pertenecientes al núcleo duro de la intimidad.

Como también se ha dicho en otros tipos penales de éste título la falta de técnica legislativa se debe principalmente a la aplicación de los ciclos o etapas del procesamiento de datos, conocido universalmente en la informática jurídica y que el constituyente de 1991, lo plasmó en el inciso 2º del artículo 15, al sostener: “En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución”. En efecto, importaba destacar el procedimiento o tratamiento informático para entender que en cada etapa se puede vulnerar derechos y libertades públicas, como la intimidad, el buen nombre, la imagen, el habeas data y la libertad de información. Sin embargo, el legislador acudió a trasplantar los fenómenos tecnológicos e informáticos que en muchas de las veces producen ajenidad con la conducta típica, antijurídica y culpable que se está estructurando; más aún podría quedar en desuso la conducta porque el fenómeno tecnológico deja en poquísimo tiempo de ser útil para transmitir y circular información y datos porque se inventa una forma mucho más versátil informáticamente hablando para transmitir imágenes, audio y texto a través del hipertexto (HTML) y la página Web contenida en ésta. Legislar los con los fenómenos tecnológicos TIC en entronque con la informática, hoy en día tiene un alto riesgo de vetustez casi inmediata. La prueba está como veremos más adelante que ni siquiera se pone en funcionamiento real la conducta penal del artículo 269 G., cuando ya existen propuestas que deambulan en el Congreso de la República, cara a reformarla.

El tipo penal mutilado o incompleto previsto en el inciso 2º, contiene los verbos modificar y acceder. El primero se utiliza para indicar que se “modifica el sistema de resolución de nombres de dominio”; y, el segundo, para significar que se hace creer a un usuario que entra en una dirección electrónica que identifica una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (*Internet Protocol*), diferente a la que él estima es la de su entidad bancaria “o sitio personal o de confianza”.

En el primer momento de este tipo penal, la utilización de los términos lleva a la confusión terminológica, ya que “modificar el sistema de resolución de nombre de dominio”, sobran los términos “el sistema de resolución de” que son equívocos y no ayudan en nada a dar claridad a la frase que debió ser “el que, modifique los nombres de dominio…”. Esto sí da claridad a la acción ilícita que se pretende, pues los nombres de dominio como se dijo antes son identificaciones electrónicas (nombres, abreviaturas, alias) ya no de la interfaz de dispositivo (IP) sino del usuario o titular informático del dominio (aunque se discute sí uno puede o no tener “propiedad” en estricto rigor jurídico y no una especie de “posesión” en la red de redes que le posibilita navegar plenamente identificado). Si alguien modifica, altera o se “apodera” de esos nombres de dominio para con base en ellos cometer actos ilícitos se encasilla en la figura penal descrita en el primer momento.

En el segundo momento del tipo penal, es acceder a un sitio de dominio diferente al que supone el usuario, pero innecesariamente el legislador penal de 2009 sólo cree que puede ser delito ingresar (o “accesar”, como incorrectamente dicen algunos) a un dominio de una entidad bancaria. Cierto es que la información financiera hoy en día es altamente sensible y puede interesar en grado sumo a los titulares de los mismos que se extravíe, pierda o

simplemente se esfume, sin más acciones que la informáticas a través de cajeros electrónicos o banca electrónica en red (que es el caso del presente punible). Sin embargo también es cierto, que hay otro tipo de información personal o perteneciente al núcleo duro de la intimidad que debería importar al legislador penal proteger y que puede hallarse no sólo en "otro sitio personal o de confianza", sino en bases de datos, sistemas informáticos o archivos informáticos de dominios privados o públicos que merecen una protección reduplicada, tal como se estila en el derecho comparado.

El tipo penal del inciso 2º del artículo 269G, es mutilado además de lo dicho anteriormente, porque su comprensión total no se entiende, si no es remitiéndose al tipo penal del artículo 269J, "transferencia no consentida de activos", al menos cuando se refiere al ingreso a un dominio diferente al que cree haberlo hecho el usuario de buena fe a un entidad bancaria, pues en cuanto a ingresar a un sitio de dominio privado o público, perfectamente tendría que remitirse al tipo penal del artículo 269 A, acceso abusivo a un sistema informático, el cual presupone una base de datos o un tratamiento de datos interconectado o no.

El privilegio de la información financiera en el derecho colombiano ha sido evidente desde los reiterados fallos de tutela de la Corte Constitucional para protegerla desde 1992 hasta nuestros, porque los tutelantes solicitaban protección judicial efectiva era porque existía una transferencia irregular bancaria, mora en los pagos, inconsistencias de los datos bancarios, desconocimiento de derechos fundamentales como la intimidad, el buen nombre, imagen, información y habeas data por datos incompletos, erróneos o falsos, etc. Precisamente eso potenció que hoy por hoy, tengamos una ley de habeas data sectorial o financiera y no una ley estatutaria de Habeas Data integral, tal como se propuso por la Defensoría del Pueblo en el año 2005.

Este privilegio de la información financiera lo recogió el legislador penal de 2009 y por eso se revela la inclinación de alta sensibilidad a éste tipo de información o datos financieros sancionados penalmente cuando se encuentra en las circunstancias del inciso 2º *in fine* del artículo 269 G.

Por su parte, el inciso 3º del artículo 269 G, plantea un tipo penal agravado de los tipos previstos en los incisos 1º y 2º y utiliza el verbo "reclutar" para indicar que el agente del delito para llevar a cabo la conducta de los tipos básicos, incorpore o enganche a "víctimas en la cadena del delito". Ese sui generis reclutamiento o enganche debería tener unas connotaciones para que esas personas (no "víctimas", pues a priori la califica el legislador): (i) que los enganchados no tengan conocimiento de la ilicitud; (ii) que su participación no sea necesaria para la consumación del ilícito; (iii) que actúe de buena fe; y, (iv) que no se considere "víctima" sino usuario de la red de redes. Tal vez, por esto eufemísticamente se le ha denominado "mula informática" o "Phisher mula" al "incauto cibernauta enganchado en una actividad ilícita que el desconoce lo sea y por tanto, se considera exento de responsabilidad penal, sí efectivamente desconoce la ilicitud de su actuación y esto en informática o el mundo "virtual", sí es posible a diferencia de la vida real.

4.7.7. El "Phishing". El artículo 1º del proyecto de ley que luego se convirtiera en Ley 1273 de 2009, consideraba que el "Phishing" era "la máscara, usualmente implementada por SPAM, mediante la que se busca apoderarse de manera ilegítima de la identidad o de los datos de una persona otorgados por un sistema de información.

"Phishing (por "fishing" pescar), proviene de cambiar la letras "f" por las dos letras : "P" y "h" que significan: "p" de password (contraseña) y la "h" de hacker (pirata informático); pues esta labor de Phising la realizan los hacker "White" and "Black".

La conducta penal del artículo 269 G., trató de trasplantar el fenómeno informático del "Phishing" tanto en la versión de apoderamiento de la identidad de nombres de dominios como de los datos personales presentes en un sistema informático, base de datos o tratamiento informático, esté en red de redes o intranet. Sin embargo, lo acondicionó no al apoderamiento que es un acto abusivo de un sistema informático, sino a la "suplantación de sitios Web" que deformó la esencia de la actividad informática y creó una conducta penal sui generis que bien pudo haberse ubicado en otras figuras delictivas como la prevista en el artículo 269 A, o en un inciso del delito de violación de los datos personales del artículo 269 F.

4.7.8. Reformar: La propuesta de reforma al delito de suplantación de sitio de Web para captar datos, previsto en el artículo 269 G, retoca la estructura de la conducta punible en los incisos 1º y 2º y elimina el 3º , pero le deja el mismo intitulado al delito. Eso sí mejora la redacción e invierte el contenido del inciso 1º y lo pone de 2º y viceversa.

En principio, se propone eliminar los términos "y sin estar facultado para ello" y se cambia el término normativo inicial que estructura el delito de "con objeto ilícito" a "con finalidad de obtener…", del inciso 1º, creemos por las razones que hemos expuesto para otros tipos delictivos del presente Título VII bis. Eso está bien. Igualmente elimina todos los verbos que aparecía en este inciso, porque aparentemente invirtió el contenido del inciso 2º , lo puso en el primero y viceversa.

La redacción se mejora en el inciso 1º que antes era el 2º, queda así: "*El que, con la finalidad de obtener datos personales y/o protegidos, mediante páginas electrónicas, enlaces o ventanas emergentes, consiga que un usuario informático acceda por error a una dirección IP distinta a la IP de un portal o Web real, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de cien (100) a mil (1000) salarios mínimos legales mensuales vigentes*".

En la nueva redacción se destaca que la finalidad del ilícito es proteger los datos personales y por el uso del término "protegidos", entendemos aquellos datos sensibles o del núcleo duro de la intimidad. Con este actuar la propuesta de reforma elimina el tipo penal mutilado que presenta el artículo 269 G, en su inciso 2º, en la propuesta inciso 1º .

Este actuar no sólo presenta el fenómeno tecnológico de la especie de apoderamiento de las páginas electrónicas y de la información contenida en ellas (de tipo textual, auditivo, imágenes y video), mediante el "acceso por error" a una dirección electrónica de IP que no le pertenece al usuario, sino la captura de datos personales o protegidos que es al fin y al cabo lo que se protege por la conducta y el Titulo VII bis del C.P.

El Inciso 2º del proyecto, sostiene: *El que diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes para la realización de cualquiera de las conductas punibles descritas en éste título, incurrirá en pena de prisión de veintiocho a cuarenta y seis meses y en multa de cien (100) a mil (1000) salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya otro delito sancionado con pena mayor*".

Convierte el antiguo inciso 1º, siendo un tipo penal básico en un inciso 2º como tipo penal agravado no sólo del tipo penal básico del artículo 269 G., sino de las seis (6) conductas típicas previstas en los artículos 269 A a, 269 F. Ahora tendría que analizarse si dicha duplicación de agravación ya se presenta en algunos tipos, o está inmersa en las causales de agravación de los tipos penales del Título VII bis prevista en el artículo 269 H. Y, esto es posible porque lo que diferencia este tipo agravado de los demás tipos básicos y agravados presentes en los artículos 269 A a 269 F., es que el presente se refiere en concreto a páginas

o portales electrónicas o sitios de Web, pues los enlaces y ventanas emergentes son vínculos e hipervínculos que posibilita una hipertexto (páginas HTML) que contiene a una página WWW o Web, y por tanto, esos tecnicismos (enlaces o *Link, o* ventanas emergentes o *Pop up*) siguen sobrando para clarificar la conducta típica, antijurídica y culpable que se piensa crear.

4.8. TIPOS AGRAVADOS CONTRA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LOS DATOS Y DE LOS SISTEMAS INFORMATICOS

En nuestro derecho penal por costumbre legislativa en los diferentes Códigos Penales siempre se han estructurado tipos penales básicos y tipos penales agravados en la misma norma jurídica.

Igualmente, se estructuran causales de agravación punitiva aplicables a todos los tipos penales ubicados en cada capítulo o título del bien jurídico protegido respectivo. Esas causales de agravación son variopintas y se fundan en aspectos, hechos o circunstancias de carácter subjetivo u objetivo adicionados o complementados a la conducta comisiva del tipo principal. El tipo penal básico tiene autonomía en la configuración de los elementos normativos que lo estructuran; en cambio, el tipo penal agravado debe su estructuración al tipo penal básico para su existencia, la configuración de éste es una consecuencia lógica y jurídica de la ocurrencia del tipo penal básico y es por eso, que el legislador penal atendiendo a esos aspectos subjetivos u objetivos adicionales con los cuales se comete el delito y lo agrava, crea unos incisos según las necesidades de tipificación agravada correspondientes.

Esta técnica legislativa se ha utilizado en los delitos contra la Información y los datos personales, en particular en cada conducta delictiva de los artículos 269 A a, 269 i del Titulo VII Bis, Capítulos I y II.

En el Capítulo I, "*De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos*", se estructuran como tipos penales básicos los siguientes: (i) Acceso abusivo a un sistema informático; (ii) Obstaculización ilegítima de sistema informático o red de telecomunicación; (iii) Interceptación de datos informáticos; (iv) Daño Informático; (v) Uso de software malicioso; (vi) Violación de Datos; y (vii) Suplantación de sitios Web para capturar datos personales

Como tipo penal agravado se estructura la Suplantación de sitios Web para capturar datos personales, cuando en la consumación del ilícito se ha "reclutado víctimas en la cadena del delito" (artículo 269 G, inciso 3º del C.P.)

En el Capítulo II, *"De los atentados informáticos y otras infracciones*", se estructuran como tipos penales básicos los siguientes: (i) El Hurto por medios informáticos, electrónicos y telemáticos; y (ii) Transferencia no consentida de activos.

Como tipo penal agravado se estructura la Transferencia no consentida de activos, cuando la conducta penal tiene una cuantía superior a 200 SMLM.

Aparte de estos tipos penales básicos y agravados, el legislador penal ha estructurado una causal de agravación punitiva para los delitos previstos en cada capítulo o título del Código Penal. Estas causales agravación en el caso de los delitos contra la información y los datos, sólo operan en los delitos que atentan la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos, es decir, los delitos de Acceso abusivo a un sistema informático; Obstaculización ilegítima de sistema informático o red de telecomunicación; Interceptación de datos informáticos; (iv) Daño Informático; Uso de software malicioso;

Violación de Datos; y Suplantación de sitios Web para capturar datos personales (artículos 269 A a 269G del C.P.).

Sin embargo, parece desproporcionada la actuación del legislador penal de 2009, cuando sólo estableció estas causales de agravación punitiva para los delitos del capítulo I, del Titulo VII Bis y no para los delitos previstos en el Capítulo II, de los "atentados informáticos y otras infracciones" que son igual o más insidiosos que los previstos en el Capítulo I, pues no solo atentan contra los datos personales, sensibles sino también los de índole financiero. Las causales de agravación debieron colocarse al final del Título VII Bis para que abarque a los dos capítulos y a todos los delitos que atentan contra la información y los datos.

Las causales de agravación punitiva [51] de estos delitos, según el artículo 269 H, son las siguientes: (i) Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros; (ii) Por servidor público en ejercicio de sus funciones; (iii) Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este; (iv) Revelando o dando a conocer el contenido de la información en perjuicio de otro; (v) Obteniendo provecho para sí o para un tercero; (vi) Con fines terroristas o generando riesgo para la seguridad o defensa nacional; (vii) Utilizando como instrumento a un tercero de buena fe; y, (vii) 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.

El legislador penal de 2009, respecto de estas causales de agravación y la estructuración de los diferentes tipos penales básicos y agravados del Título VII Bis, cometió una reiteración, como mínimo de tipos penales (básicos y agravados) conjuntamente con causales de agravación punitiva que en determinados casos concretos el juez competente deberá saber cuál de ellas aplicar o si por el contrario se estaría violando el llamado principio del *ne bis in ídem,* si da aplicación al tipo penal básico y/o agravado y además la causal de agravación.

Es el caso por ejemplo del tipo penal básico denominado "violación de datos personales", previsto en el artículo 269 F del C.P., que se estructura *ab initio* con los elementos normativos del tipo "…con provecho propio o de un tercero…" y la causal de agravación punitiva 5ª del artículo 269 H., aplicable a este tipo penal básico es: "Obteniendo provecho para sí para un tercero", con lo cual existe una reiteración de las conductas comisivas que en el mejor de los casos, solo se deberá aplicar la figura penal básica sin la agravante, pues el tipo penal básico ya está configurado como tipo penal agravado.

---

(51) Según ***la Sentencia C-038-1998,*** la Corte Constitucional sostuvo: *"Desde el punto de vista material la norma no consagra una causal de agravación punitiva que pueda tildarse de injusta o discriminatoria, ya que, si bien hace más difícil la situación de ciertas personas ante la aplicación de la ley penal, no lo establece así gratuitamente sino a partir de diferencias relevantes que precisamente llevan a considerar que, dentro de la sociedad, los individuos de quienes se trata son precisamente los "distinguidos", esto es, los que sobresalen por cualquiera de los factores enunciados, colocándolos en un nivel privilegiado frente a los demás. Es precisamente de ellos -a quienes más se ha dado- de quienes más se espera en lo relativo a la observancia de la ley y el respeto al orden jurídico. No puede ser mirada ni evaluada en la misma forma por el legislador ni por el juez la conducta de un individuo común que la de aquél que, precisamente por su puesto dentro de la escala social, tiene una mayor responsabilidad hacia el conglomerado y a quien se mira por muchos como paradigma y guía de conducta. Si, no obstante su jerarquía o su importancia, vulnera las reglas de convivencia, con mucho mayor conocimiento acerca del daño que su comportamiento causa, es natural que se le aplique una mayor severidad en el juicio y en la tasación de la pena".*

Iguales argumentos se presenta con el tipo penal agravado de suplantación de sitios web para capturar datos personales, cuando para consumarlo el agente "ha reclutado víctimas en la cadena del delito", previsto en el artículo 269 G, inciso 3º del C.P. La causal de agravación 8º , reza: "utilizando como instrumento a un tercero de buena fe". Aunque los términos empleados sean diferentes la esencia de la actuación de esos "terceros" o "víctimas" es idéntica y aquí observamos otra reiteración de tipificación delictiva, o acaso una violación al principio del Ne bis in ídem.

La Corte Constitucional en la sentencia C-870-2002, compiló la jurisprudencia constitu- cional sobre aquél principio, expresó que: "*El principio non bis in ídem prohíbe que una persona, por el mismo hecho, (i) sea sometida a juicios sucesivos o (ii) le sean impuestas varias sanciones en el mismo juicio, salvo que una sea tan solo accesoria a la otra"*

4.9. DELITOS PREVISTOS EN EL CAPITULO II, DEL TITULO VII Bis del C.P.

4.9.1. HURTO POR MEDIOS INFORMATICOS "Y SEMEJANTES"

4.9.1.1. Fuente Normativa: Artículo 269 I. concordante con los artículos 239 y 240 del C.P., relativos al delito de Hurto.

4.9.1.2. El tipo penal. *El que, superando medidas de seguridad informáticas, realice la conducta señalada en el art. 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurra en las penas señaladas en el artículo 240 de este código*.

El legislador penal de 2009, intitular el delito de hurto por medios informáticos "y semejantes" debió ser más concreto y especificar que se trata del delito de hurto por medios informáticos, electrónicos y telemáticos, que son los únicos posibles de semejanza con los informáticos actualmente, máxime que la ley penal ha aceptado que los medios informáticos, electrónicos y telemáticos son circunstancias de mayor punibilidad en el artículo 58 de la parte general del Código Penal.

4.9.1.3. Ubicación del tipo penal. En el Título VII Bis: *"De la protección de la Información y los datos"* personales, **Capitulo II.** *"De los atentados informáticos y Otras infracciones".*

En una de los propuestas de reforma al C.P., y la creación del Título VII Bis [52], referido a los delitos contra la información y los datos, se proponía además de elevar a conducta delictiva el hurto por medios informáticos y semejantes, la falsedad informática [53], la transferencia no

---

(52) Nos referimos a la propuesta presentada a la Comisión Primera Constitucional del "Texto aprobado en Comisión Primera de la Cámara de representantes del proyecto de Ley números 042/07, Cámara acumulado con el 123/07, Cámara "Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado –denominado "De la protección de la información y de los datos"—y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". Vía Internet.

(53) **La propuesta inicial de reforma al C.P., del Juez Segundo Promiscuo Municipal de Rovira (Tolima), Alexander García, sostenía. ARTÍCULO 269I: Falsedad informática.** El que sin autorización para ello y valiéndose de cualquier medio electrónico, borre, altere, suprima, modifique o inutilice los datos registrados en una computadora, incurrirá en prisión de cuatro (4) a ocho (8) años y en multa de 50 a 500 salarios mínimos legales mensuales vigentes. La propuesta presentada a la Comisión Primera Constitucional ya se cambiaba así: FALSEDAD INFORMATICA. El que, sin estar facultado para ello, introduzca, altere, borre, inutilice o suprima datos informáticos, generando datos no auténticos, con la finalidad de que sean percibidos o utilizados a efectos legales como genuinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

consentida de activos, el espionaje informático [54], la violación de reserva industrial o comercial valiéndose de medios informáticos [55]. Después de expedida la Ley 1273 de 2009, se ha propuesto la creación del delito de "*enmascaramiento ilícito*" [56]

4.9.1.4. Sujetos de la conducta penal. El delito de hurto por medios informáticos y semejantes, tiene como sujeto activo a personas particulares como a servidores del Estado.

Sujetos pasivos del ilícito será el Estado, pero también personas naturales o jurídicas que administren, coordinen o dirijan bases de datos, sistemas informáticos o sistemas de tratamiento informático, o bien sean operadores o fuentes de información, a tenor de la ley 1266 de 2008.

4.9.1.5. Conceptualizaciones. El artículo 269i del C.P., trae varios términos técnico-informáticos para la construcción del tipo penal mutilado de dos actos (remisiones al artículo 239 y 240 del C.P, sobre estructuración del tipo básico de hurto y las sanciones impuestas al mismo).

Los términos siguientes términos aparecen en el artículo 1º del proyecto de ley de la que luego fuera la Ley 1273 de 2009 y ésta se eliminara dicho artículo que traía estas definiciones:

La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Sistema electrónico: Es un conjunto de circuitos que interactúan entre sí para obtener un resultado.

Sistema telemático: Es el formado por equipos informáticos interconectados por una red de comunicaciones o telecomunicaciones que, a su vez, está constituida por circuitos, equipos de transmisión y equipos de conmutación.

Sistema de autenticación: Cualquier procedimiento que se emplee para identificar, de manera inequívoca, a un usuario de un sistema informático.

---

(54) **Articulo 269L. *Espionaje informático.*** El que, sin estar facultado para ello, se apodere, interfiera, transmita, copie, modifique, destruya, utilice, impida o recicle datos informáticos de valor para el tráfico económico de la industria, el comercio, o datos de carácter político y/o militar relacionados con la seguridad del Estado, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes, siempre que la conducta no esté castigada con una pena mayor.

(55) **Artículo 269M. *Violación de reserva industrial o comercial valiéndose medios informáticos.*** El que, sin estar facultado para ello, realice una cualquiera de las conductas señaladas en el artículo 308 de este Código, valiéndose de medios informáticos y superando las seguridades existentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales, siempre que la conducta no esté castigada con una pena mayor.

(56) ***Enmascaramiento ilícito*** (IP *spoofing*). El que, sin estar facultado para ello, con el propósito de obtener provecho ilícito para sí o para un tercero o para usar y disfrutar servicios informáticos a los cuales no tiene derecho o para causar daño, sustituya o suplante a otro o se atribuya una identidad informática o una calidad que pueda tener efectos jurídicos, incurrirá en pena de prisión de veintiocho (28) a cuarenta y seis (46) meses y en multa de cien (100) a mil (1000) salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya otro delito sancionado con pena mayor.
Las penas señaladas en el inciso anterior se aumentarán hasta en la mitad, cuando se realicen dichas conductas con fines terroristas o de carácter extorsivo".

4.9.1.6. El Hurto informático: un delito mutilado de dos actos.

El delito de "hurto por medios informáticos", electrónicos o telemáticos, al interpretar "u semejantes" (artículos 269 i y 58 del C.P.), es un tipo penal mutilado de dos tiempos. En un primer momento, porque para su construcción se debe contar esencialmente con la estructura del delito de hurto simple previsto en el artículo 239 del C.P.; y en su segundo momento, en cuanto a la dosimetría punitiva de la sanción debe ha de contarse con las sanciones previstas en el artículo 240 del C.P.

Por estas razones, existía una postura de asimilación de la conducta a los tipos penales existentes de hurto y hurto calificado; y otra devenida de alguno de los ponentes del proyecto de ley, que luego fuera la Ley 1273 de 2009, que propugnaba por la eliminación de la propuesta del hurto por medios informáticos.

En efecto, sobre la primera postura se dice que según la redacción del artículo 269i, parece que más fácil hubiese sido adicionar el artículo 239 relativo al delito de hurto, adicionando un tipo penal agravado que recoja las acciones previstas en el artículo 269 i, como son: *"manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, …*", y dejando el tipo penal básico del hurto, es decir, "*el que se apodere de una cosa mueble ajena, con el propósito de obtener provecho para sí o para otro*"; o incluso adicionar un numeral al artículo 240, relativo al delito de hurto calificado, cualquiera de las dos opciones, pero no como se procedió en aras de proteger el bien jurídico de la información y los datos, en la conducta penal del articulo 269i, en el Titulo VII bis. Esto por cuanto, en la redacción no queda claro que el agente de la conducta se quiera apropiar de los datos personales contenidos en un sistema informático, electrónico o telemático "u otro semejante", sino que habla de maniobras indebidas: manipulación o suplantación de "sistemas de autenticación y de autorización establecidos" que típicas acciones de daños informáticos más que de acciones de apropiación o hurto informático.

El término clave que debió aparecer con determinante del delito debió ser "el dato personal", porque ese es el objeto mueble intangible ajeno susceptible de apropiación y no los sistemas informáticos y demás medios informáticos, electrónicos o telemáticos compuestos por elementos físicos o de hardware o lógicos, programas de computador o software, pues la apropiación de éstos podría constituir un delito de hurto simple o calificado según los elementos constitutivos y acciones humanas contra dichos elementos, o en casos excepcionales de delitos contra la propiedad intelectual si se apoderan de los derechos morales contenidos en los programas de computación; pero en todo caso, nada tendrían que ver con el delito de "hurto informático" aquí previsto.

Por eso, la estructuración de este delito tiene serios reparos, por los mismos ponentes del proyecto de reforma al C.P [57]. En efecto, planteaba entre otras cosas, que la conducta penal ya estaba prevista como hurto agravado en el numeral 4º del artículo 240, al decir: "… *llave…falsa, ganzúa o cualquier otro instrumento similar, o violando o superando seguridades electrónicas u otras semejantes*".

Efectivamente, los términos "llaves falsas" entre otras, son "*las tarjetas electrónicas, tarjetas perforadas y los mandos o instrumentos de apertura a distancia*" (artículo 239 in fine del C.P. Español de 1995. Igualmente, se dice que se comete el delito de hurto "*violando o superando seguridades electrónicas o semejantes*". Las medidas de seguridad electrónica son todos

---

(57) Ponencia del Senador Parmenio Cuellar Bastidas en l***a Comisión Primera Constitucional del Senado. Congreso de la República***, Bogotá, Mayo 14 de 2008.

aquellos dispositivos de físicos o lógicos computacionales que no permiten el acceso, mantenimiento, transmisión o flujo de informaciones o datos personales, para quien no está autorizado o reconocido debidamente mediante claves, contraseñas, “login”, “IP”, etc.

En ambos casos, está perfectamente previsto el hurto informático, independiente que el apoderamiento de datos o informaciones se realice con medios informáticos, electrónicos o telemáticos que son considerados agravantes del tipo penal y que hoy por hoy, son las nuevas tecnologías TIC, aplicadas conjuntamente con la informática.

4.9.1.7. Reforma. La propuesta de reforma al artículo 269i, hurto por medios informáticos, electrónicos o telemáticos, sobre el particular no se pronunció pues lo dejó en las mismas condiciones de estructuración y tipificación inicialmente planteadas.

Sin embargo, debió aprovecharse esta oportunidad para mejorar la redacción y adecuarlo al bien jurídico tutelado de la información y los datos, pues tal como está redactado, existe una ajenidad evidente por que más parece que se protegieran los bienes muebles físicos o de hardware e incluso los de software, que la información o datos personales o sensibles o del núcleo duro de la intimidad.

En el Código penal español de 1995, se estructuró el tipo penal de “apoderamiento subrepticio de documentos o efectos personales” (art. 197-1), que incluye papeles, cartas, mensajes de correo electrónico “o cualesquiera otros documentos” (v.gr. documentos electrónicos, informáticos y telemáticos), que contienen datos personales y dirigidos a vulnerar la intimidad y la propia imagen, con lo cual se observa que el bien jurídico protegido son los derechos fundamentales de la persona por el descubrimiento de la confidencialidad o el secreto que contienen dichos datos personales.

Sin embargo, en nuestro medio al revés nos preocupamos por estructurar los llamados delitos informáticos atendiendo al fenómeno tecnológico, la estructura, su funcionalidad y los efectos que produce en las acciones humanas y por ello la lluvia de críticas de quienes sostienen que los medios informáticos, electrónicos y telemáticos deben permear todas las actividades de la vida cotidiana pero no desplazar la actividad humana que se sirve de aquellos. El Código Penal debe regular conductas humanas que se consideran ilícitas sea cual fuere los medios que se utilice y no viceversa.

4.9.2. DELITO DE TRANSFERENCIA NO CONSENTIDA DE ACTIVOS

4.9.2.1. Fuente Normativa: Artículo 269 J., del C.P.

En alguna ponencia ante la Comisión Primera del Senado () el ilícito de “transferencia no consentida de activos” se manifestó eufemísticamente: “*este artículo es simplemente un **hurto agravado** por el numeral 4º del artículo 240 en relación con el artículo 239 del C.P.*”

El Convenio de Budapest de 2001, recomendó a los Estados Miembros de la UE, elevar a conducta delictiva “*los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante: a) cualquier introducción, alteración, borrado o supresión de datos informáticos, y b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona*”.

Esta tipificación de fraude informático subsume el tipo penal de transferencia no consentida de activos y plantea otras posibles conducta que se hallarían inmersas dentro de las premisas terminológicas del tipo, pues no se concentra en el fenómeno de transmisión de datos

financieros sino muchos antes en el sistema de tratamiento informatizado de datos, o sea, desde el acceso (introducción), alteración, borrado o supresión de datos que se dan en la etapa de recolección, almacenamiento, registro y circulación de datos.

4.9.2.2. El tipo penal. *El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 SMMV.*

La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 SMMV, la sanción allí señalada se incrementará en la mitad.

El "fraude informático" para los Estados Europeos que siguen las directrices del Convenio de Budapest de 2001, plasmadas en el artículo 8º, o la *"Estafa informática*" mediante manipulaciones informáticas de hardware y software, para el Derecho español, o el "*Hurto agravado*" con medios electrónicos, informáticos o telemáticos, para uno de los ponentes del proyecto de ley, previo a la Ley 1273 de 2009 (), el Código Penal Colombiano, reformado en 2009, instituyó esta figura penal como transferencia no consentida de activos en el artículo 269 J, bajo el bien jurídico de la información y los datos y en protección contra los "atentados informáticos y otras infracciones".

El fraude informático propuestos en el Convenio de Budapest, tiende a proteger los datos personales con relevancia patrimonial, igual al objetivo que persigue el delito de transferencia no consentida de activos del derecho colombiano; en cambio, en el ámbito español el bien jurídico tutelado es el patrimonio y el orden económico social, pero con una aclaración que la estafa informática es un de carácter específico y en donde se persigue los resultados materiales finales no por el engaño a otra persona, sino a través de la manipulación informática o el engaño virtual producido a los dispositivos computacionales (físicos o de hardware y/o lógicos o de software).

4.9.2.3. Sujetos de la conducta punible. Por la utilización de los términos "El que, …", en el tipo penal, se entiende que puede ser sujeto activo toda persona particular o servidor del Estado entendiendo que en éste último caso, la agravación de la punibilidad sobrevendrá por las causales previstas en la parte general del Código Penal, previstas en el artículo 58.

Sujeto pasivo de la conducta será el Estado, pero al igual que otras conductas penales del Título VII bis, también lo podrán ser personas naturales o jurídicas, particulares o públicas, así como los administradores de bancos de datos personales y financieros (bancarios, de corporaciones de ahorro, tributarios, fiscales y de valores de bolsa) y operadores de información, Directores de Agencia de información comercial, en los términos que estipula la Ley 1266 de 2008 o ley de Habeas data financiero.

4.9.2.4. El Delito de transferencia no consentida de activos. El artículo 269 J del C.P. estructura el tipo penal básico en los siguientes elementos normativos: (i) El ánimo de lucro; (ii) la manipulación informática o artificio semejante; y (iii) la transferencia no consentida de "cualquier activo" en perjuicio de un tercero.

Estos tres elementos son consecutivos para que la conducta de resultados se produzca, aunque el elemento del consentimiento bien pudo haberse omitido por estar regulado en la parte general del Código Penal al mencionar la antijuridicidad de la conducta.

El provecho económico es un elemento de la esencia del tipo, pues al ser una conducta de resultado se entiende que debe estar previsto para que se configure el tipo penal.

Respecto de las "manipulaciones informáticas", se entiende toda alteración o modificación de datos, ya sea suprimiéndolos, introduciendo datos nuevos y falsos, colocar datos en distinto momento o lugar, variar las instrucciones de elaboración, etc.

"Se diferencia en las estafas informáticas de las cometidas dentro del sistema y las cometidas fuera del sistema. Las primeras son las manipulaciones realizadas directamente sobre el sistema operativo y no existe ningún engaño ni error sobre un ser humano. Las estafas cometidas fuera del sistema, son las manipulaciones de datos hechas antes, durante y después de la elaboración de los programas, siendo éstas las causantes del engaño que determina de disposición patrimonial" **[58]**.

Por la ubicación y bien jurídico protegido ("la información y los datos") del delito de transferencia no consentida de activos, las manipulaciones informáticas que se presentan en los datos es aplicable a la conducta penal mencionada en el derecho colombiano.

4.9.2.5. Visión integracionista de conductas penales vistas en la "transferencia no consentida de activos".

En cuanto a la "**transferencia no consentida de activos**", ocurre por una de tres razones: *torpeza, exceso de confianza* o *novatada* de quien ingresa con su computador a la red.

Normalmente esa transferencia no consentida va precedida de la aceptación del dueño del computador conectado a la **Internet** (potencial víctima)**,** que acepta recibir el archivo que contiene encriptado el programa malicioso (**malware**), o que desestima imprudentemente el consejo de no aceptar comunicación con quien no conoce, y no abrir mensajes de correo electrónico provenientes de direcciones desconocidas (evita el **hacking**), o que desecha la recomendación de digitar en el navegador, directamente y tantas veces como sea necesario, el nombre de la página que desea visitar (la página del banco, por ejemplo) en lugar de apelar al recurso de "completado automático de direcciones" o sitios web, aplicación que ofrecen la mayoría de los navegadores (Internet Explorer, Opera, Motzilla, Netscape), así como de los sistemas operativos, ya sean pagados (como Windows-DOS, Windows-MAC, etc.) o gratuito, llamado comúnmente "software libre", que es Linux; y caen en la "*suplantación de sitios web***"**, *(phishing)* dotados de apariencia similar a la de la entidad que se desea visitar, y donde se digitan las claves personales de cuentas bancarias que luego son utilizadas para hacer transferencias de dinero a otras cuentas **[59]**.

4.9.2.6. Tipo Básico de transferencia valores económicos (Defraudaciones y estafa): (i) Transferencia no consentida de activos por manipulación informática o artificios semejantes (hardware); (ii) Transferencia no consentida de activos por manipulación de software de

---

(58) AA.VV. ***Inclusión de los delitos informáticos dentro del Código Penal del Estado***. En: www.monografías.com

(59) Informe de ponencia para primer debate al Proyecto de Ley 281 de 2008 Senado, "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "De la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías en la información y las comunicaciones, entre otras disposiciones"

computador. “Estafa Informática o telemática”

En el Código Penal Español de 1995, se elevó a conducta penal “*las manipulaciones informáticas dirigidas a conseguir una transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero*” (artículo 248-2), como una forma de delito de estafa y bajo el Capítulo VI, De las defraudaciones y el Título XIII de los delitos contra el Patrimonio y el Orden Económico Social.

“*Nos encontramos frente a un tipo defraudatorio que no comparte la dinámica comitiva de la estafa tradicional y, en consecuencia, ajeno a la elaboración doctrinal y jurisprudencial de los elementos esenciales que la configuran. Es más, no solo se trata de constatar que el concepto general de estafa no ejerce aquí una función de criterio rector interpretativo de las conductas penalmente relevantes, sino que, precisamente esa ha sido la ratio legis del precepto: criminalizar conductas lesivas para el patrimonio ajeno extramuros de la dinámica comitiva presidida por el engaño*”

“Con todo y con ello, debe tenerse en cuenta que la nueva figura presenta importantes similitudes con la estafa. En efecto, el bien jurídico protegido es el patrimonio, y no por tanto, tan solo la posesión o la propiedad de cosas muebles ajenas. La transferencia a cualquier activo patrimonial como objeto material sobre el que deba recaer la acción típica así lo avala. Por otra parte, la actividad comitiva a través de manipulaciones informáticas tiende a conseguir una ´transferencia´ no consentida de activos patrimoniales. Es decir, si bien es evidente que no supone la provocación de un acto de disposición viciado como medio de ataque al patrimonio probablemente deban descartarse las conductas de sustracción de algún elemento integrante del mismo.

“…el fraude informático regulado en el apartado 2º del artículo 248 CP no contempla las hipótesis de sustracción de dinero a través de la utilización no autorizada de tarjetas magnéticas sobre los denominados ´cajeros automáticos´…no se trata de transferencia de activos patrimoniales, sino de sustracción de dinero mediante el uso por un tercero del medio específico adecuado para acceder al mismo…”

“En definitiva, la criminalización de las manipulaciones informáticas tendentes a provocar la transferencia no consentida de cualquier activo patrimonial… nos encontramos ante una estafa específica, ajena al concepto general” de estafa, es “un tipo penal de resultado material que exige para su consumación el efectivo perjuicio económico en el patrimonio ajeno, a través de la transferencia no consentida de un determinado activo patrimonial...[60].

4.10. A manera de colofón

1. Se adiciona un nuevo Título (VII Bis) al Código Penal de 2000 que protege “**La información y los datos” personales**, los cuales parcialmente se habían regulado en el Capítulo VII, “Delitos contra la Intimidad, reserva e interceptación de comunicaciones (art. 192 a 197) del Título III, “Delitos contra la libertad Individual y otras garantías”.

2. La confidencialidad, la integridad y la disponibilidad de los datos personales son principios o características intrínsecas del derecho a la Intimidad que se materializan en el ejercicio del Habeas Data.

---

(60) QUINTERO OLIVARES, Gonzalo. ***Delitos contra el patrimonio y el orden económico social. Comentarios a la parte especial del Derecho Penal.*** Ed. Aranzadi, Pamplona, 1997, p. 489

3. Se crea un bien jurídico específico de la **Información y los datos personales** del género Habeas Data.

4. Se traslada el delito "**acceso abusivo a un sistema informático**" contra la intimidad (art. 195) a tutelar la Información y los datos (art. 269 A), en este nuevo Titulo.

5. Se penaliza todas las fases del proceso informático desde el acceso, almacenamiento y registro de la información hasta la circulación, transmisión o comunicación informática, electrónica y telemática de los datos personales.

6. El Capitulo II del Titulo VII Bis, **resulta exótico en la ubicación que le asigna**, a no ser porque la informática se toma como "medio" para consumar los tipos delictivos de Hurto y de transferencia no consentida de activos, pues mejor ubicados estarían en los delitos contra el Patrimonio Económico, pues estos son delitos de resultado.

7. Se eliminaron en el texto definitivo de la ley, **las definiciones de los términos técnicos** que utilizan los diferentes tipos por ajenidad jurídica de la norma.

8. Se establecen unas **causales de agravación punitiva** para los delitos del título VII Bis: (i) Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros, (ii) Por servidor público en ejercicio de sus funciones, (iii) Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este, (iv) Revelando o dando a conocer el contenido de la información en perjuicio de otro, (v) Obteniendo provecho para sí o para un tercero, (vi) Con fines terroristas o generando riesgo para la seguridad o defensa nacional, (vii) Utilizando como instrumento a un tercero de buena fe, y (viii) 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.

9. Se establecen **penas** de prisión que van desde los treinta y seis (36) hasta los ciento veinte (120) meses y multas de 100 a 1.000 salarios mínimos legales mensuales vigentes, según el tipo delictivo básico.

10. Se relacionan tipos delictivos básicos y agravados de **carácter doloso no culposos**. Así mismo delitos alternativos o consecutivos, según la forma copulativa o disyuntiva de los verbos rectores.

11. Los tipos delictivos del presente título son de **conocimiento de los "jueces municipales**" según los procedimientos generales previstos en el C.P.P. Se eliminó un procedimiento especial que preveía en el anteproyecto de la Ley 1273.

12. El Sector **financiero y económico** público y privado, como las **entidades estatales** en nuestro país son los más beneficiados con la tipificación de estas conductas delictivas

BIBLIOGRAFIA GENERAL

AA.VV. ***Inclusión de los delitos informáticos dentro del Código Penal del Estado***. En: www.monografías.com

AA.VV. ***Informe de ponencia para primer debate al proyecto 281 de 2008***. Senador Parmenio Cuellar . Bogotá, Mayo 14 de 2008, p. 5.

AA.VV. ***Ley sobre protección a la vida privada o protección de datos de carácter personal***. En: http://www.sernac.cl/leyes/

CASTRO OSPINA, SANDRA J. ***La información como bien jurídico y los delitos informáticos en el nuevo Código Penal Colombiano.*** Universidad Externado de Colombia, Bogotá, Julio 15 de 2002. Vía Internet.

JARVLEPP, Harry. B.A., LL.B., M.B.A. ***Information technology and new media law***. En: ***KnowledgeBase. An information Technology Law Bulletin***- Fall 1997. En: WWW.Umontreal.edu.ca

KATSH, *Ethain.* ***Rigths, camera, action****. O*b. ut supra cit. En: WWW.UMONTREAL.EDU.CA

LIVELLARA, Silvina. ***Hábeas Data e información crediticia. La eventual responsabilidad civil de las entidades financieras y del banco central de la República argentina por cesión y publicidad de datos inexactos****.* Vía Internet.

MORALES PRATS, Fermín. ***Comentarios a la parte especial del Derecho penal. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio***. Ed. Aranzadi, Pamplona (España), 1997

MITNICK, Kevin, SIMON, William L. ***El arte de la intrusión. Cómo ser un hacker o evitarlos.*** Editorial Alfaomega Ra-ma, 1ª ed., 2007.

HERNANDEZ, Jaime A. y VARGAS, Javier. ***Pliego de modificaciones al proyecto de ley Estatutaria 201 de 2003 y 071 de 2002 Senado***. Ponentes del proyecto acumulado. Vía Internet.

OLIVARES QUINTERO, Gonzalo. ***Comentarios a la parte especial del Derecho penal. Delitos contra el Patrimonio y el Orden Económico Social***. Ed. Aranzadi, Pamplona (España), 1997

PALAZZI, Pablo. ***El Hábeas Data en el derecho argentino****.* Revista de Derecho Informático. ISSN 1681-5726. Ed. Alfa-Redi, No. 04, Noviembre de 1998.

PUCCINELLI, Oscar. ***El Hábeas Data en el Brasil****.* En: www.astrea.com

Riascos Gómez, Libardo Orlando. ***El habeas data: Visión constitucional, legal y punitiva****. Ed. UNED, Universidad de Nariño. ISBN: 978-958-8609-08-9,* Pasto, 2011

_____ ***La Constitución de 1991 y la Informática Jurídica***. Ed. UNED, Universidad de Nariño, Pasto, 1997

_____***El habeas Data: Visión Constitucional, visión legal y en proyectos de ley estatutaria***. En publicación, Universidad de Nariño, Pasto, 2009

_____ ***EL derecho a la Intimidad, la visión ius-informática y los delitos relativos a los datos personales.*** Tesis Doctoral, Universidad de Lleida (España), Lleida, 1999

_____ ***Los datos personales informatizados en el derecho foráneo y colombiano*****. Análisis de las fases del Proceso Informático.** En: http://akane.udenar.edu.co/derechopublico.

CYBERGRAFIA

http://www.superfinanciera.gov.co/GuiasInformativas/educa-centralesriesgo.htm
http://es.wikipedia.org/wiki/Telecomunicaci%C3%B3n. Enciclopedia WIKIPEDIA.
http://es.wikipedia.org/wiki/Bulo.
http://es.wikipedia.org/wiki/Contrase%C3%B1a
http://es.wikipedia.org/wiki/Dominio_de_Internet
http://es.wikipedia.org/wiki/Direcci%C3%B3n_IP
http://akane.udenar.edu.co/derechopublico