ENSAYO JURÍDICO DE DERECHO INFORMATICO

DERECHOS FUNDAMENTALES, INFORMATICA Y NORMAS PENALES

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

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

ABSTRACT

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

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

ABSTRACT

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

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

CONTENIDO

PARTE PRIMERA

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

Primera postura: No existe el delito informático
Segunda postura: Posición ecléctica
Tercera postura: El delito informático existe doctrinalmente
Cuarta postura: Clasificación del delito informático, en especial, los que atentan contra la intimidad.
Clasificaciones guiadas por el derecho alemán. El bien jurídico tutelado: la información.
Clasificaciones del delito informático en donde uno de los bienes jurídicos más importante, a proteger es la intimidad.

DESARROLLO

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 priorizarse, casi única y exclusivamente con base en las convencionales delincuencias de "sangre", las "patrimoniales" o cualquiera otra que atentara contra un bien jurídico protegido y protegible tradicionales, tal y como se puede constatar con la simple lectura de los diversos catálogos punibles de los Estados modernos incluídos 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 ius-penalistas, 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 multitratamiento de la información y la comunicación por medios electrónicos, por el avance y gran poder de la tele-transmisión 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, tal como hemos analizado en los documentos electrónicos denominados: LA VISION IUS-INFORMATICA

DEL DERECHO A LA INTIMIDAD, NO ES UN NUEVEO DERECHO FUNDAMENTAL y LOS DATOS PERSONALES INFORMATIZADOS EN LA LEGISLACIÓN FORÁNEA Y COLOMBIANA, 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 su puesto, 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. artículos 18 y 20.1.d), CE., y artículos 15 y 20, Constitucionales colombianos). Hoy por hoy, en la llamada *era de la informática*, el derecho de acceso a la información adquiere relevancia capital que oscila entre el mayor o menor grado de poder de control sobre los datos o informaciones que conciernen a las personas cuando se hallen almacenados, registrados, conservados o transmitidos por medios informáticos, electrónicos o telemáticos por personas naturales, jurídicas, públicas o privadas, según fuere el caso. En dicho marco, se produce el binomio derecho-protegido y derecho-vulnerado y el correspondiente equilibrio ponderado que deviene principalmente de los límites constitucionales y legales de los derechos y libertades fundamentales en éste involucrados y que tanto hemos comentado a lo largo esta investigación.

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

En efecto, así se ha procedido en el Canadá al emitir leyes que regulan los derechos de acceso a la información y el derecho a la intimidad (Access to information Act, 1980-1983; Privacy Act 1980-83), igual en Australia (Freedom of information Act 1982, complementada por la Privacy and Data Protection Bill, 1994 -NSW- , Privacy Act, 1988) [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 LORTAD, L.O.5/92, Oct. 29. 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, artículos. 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 extra-penal" [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".

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 Título VI "Invasion Privacy" (artículos 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 (artículo 184); 2. Interceptación de datos consentida por una de las partes (artículo184.1 y 2) y/o por telecomunicaciones u otros medios tecnológicos (artículo184.3); 4. Interceptación judicial de datos en circunstancias excepcionales (artículo 184.4); 5. Interceptación de datos o información a través de dispositivos electromagnéticos, mecánicos o telemáticos, con fines de lucro (artículo 184.5); 6. Interceptaciones autorizadas (artículo 185); 7. Interceptación por autorización judicial. Excepciones. (artículo186); 8. Interceptación de un dato o información secreta o confidencial. Agravantes (artículo 187); 8. Interceptación por autorización judicial en casos especiales (artículo 188); 9. Posesión o compraventa de dispositivos electromagnéticos o informáticos utilizados en la interceptación subrepticia de datos. (Artículo 191); 10. Descubrimiento o revelación de la información sin consentimiento con medios mecánicos, informáticos o electromagnéticos (artículo 193); y, 11. Descubrimiento de datos o informaciones interceptadas, sin consentimiento, a través de medios electromagnéticos, mecánicos e informáticos (artículo 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, Título. X, del Código Penal Español del 95 (artículos. 197 a 201), en forma prolija estudia la terminología técnica, jurídica e informática empleada en la regulación de las "infracciones administrativas" previstas en la LORTAD (artículo 42 y siguientes) y los delitos del artículo 197.2, pues a su juicio, la LORTAD gana en identificación y precisión terminológica, de la que adolece el código penal, a tal punto que causa "incertidumbre" y " parece que el desconcierto y la precipitación han precedido la creación de éste precepto" (artículo197).

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 LORTAD en el ciclo operativo del banco de datos". *Arroyo Zapatero* [12], en esta mima 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 ius-administrativa.

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, artículos. 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 prevé una y otra clasificación [16] .

Las formas típicas del derecho alemán son: 1. Espionaje de datos (Artículos. 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 Código Penal de 1980, no tiene referencia expresa, pero sí tácita al derecho de *Habeas Data* y/o a la intimidad como bienes jurídicos protegibles de cualquier atentado por parte de la informática o telemática dentro del género del bien objeto del Título X, "De los Delitos contra la Libertad Individual y otras garantías". En efecto, dos razones convincentes nos llevan a sostener este argumento: por una lado, debemos tener en cuenta que en una etapa de la evolución de los derechos fundamentales, éstos retomaron la configuración, estructura y contenido de las viejas "libertades constitucionales" del liberalismo clásico y post-industrial anglo-francés a la que no escaparon el habeas data y la intimidad, y por otro lado, tanto el derecho de *habeas data* como la intimidad o "privacy", tienen hoy una identidad propia en la Constitución Colombiana de 1991 (artículo15), a pesar de que el Código Penal todavía mantiene ese origen nominativo y genérico de "Libertades Públicas" como bien jurídico protegible penalmente para referirse a una variopinta gama de derechos hoy considerados fundamentales dentro de los que están los mencionados.

En efecto, la Constitución, en el Titulo II, "De los derechos, las garantías y los deberes", Cap. I. "De los Derechos Fundamentales", artículo 15, "Derecho a la intimidad personal y familiar", constitucionaliza los derechos a la intimidad y el *habeas data,* al fusionarlos en un mismo artículo, bajo la fórmula siguiente: " *Todas las personas tienen derecho a su intimidad...Del mismo modo, tiene derecho a conocer, actualizar y rectificar las informaciones...*" entendiendo el constituyente del 91, que éste último es una consecuencia lógica de la estructuración de la intimidad y no otro derecho también fundamental que tiene su sustento en el derecho a la información (artículo20 y 73 ibídem), en el desarrollo de la personalidad (artículo 16 id.) y en los valores constitucionales de la dignidad, respeto y solidaridad humanos (artículo 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 (Sent.T-022, Ene. 29/92).

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

Sin embargo, para seguir el hilo de este aparte digamos que el actual Código Penal de 1980, bajo el concepto genérico de libertades públicas subsume a la intimidad como bien jurídico protegible de cualquier conducta humana que utilice medios electromagnéticos, computacionales o telemáticos en el Título X, Capítulo V., del Código Penal Colombiano., al referirse a los delitos de "violación de secretos y comunicaciones", y en concreto, a: 1. La "violación ilícita de comunicaciones" (artículo 288); y, 2. La "violación y empleo de documentos reservados" públicos o privados. Así mismo, por los delitos previstos en la legislación especial Decreto Ext. 2266 de 1991: "utilización ilícita de equipos transmisores o receptores", incluidos los "electrónicos" --informáticos o telemáticos--, (artículo16), y "interceptación ilícita de correspondencia oficial" (artículos. 18) . La honra (artículo 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 (artículos 313 y siguientes del C.P. Col,), al estar incorporados en el bien jurídico tutelado de "la Integridad Moral".

En el nuevo Código Penal Colombiano (Ley 599 de 2000, Julio 24), que entrará a regir dentro de un año (artículo 476), se prevé, por primer vez en Colombia en forma expresa la protección del derecho constitucional a la intimidad, dentro de los "Delitos contra la Libertad Individual y otras garantías", en el capítulo VII, "De la violación a la intimidad, reserva e interceptación de (las) comunicaciones" [16A]. En dicho capítulo se prevé en forma expresa los diversos tipos delictivos que atentan la intimidad tanto por medios y técnicas tradicionales como por medios electrónicos, informáticos o telemáticos. En tal virtud, una vez entre a regir nuestro Código Penal de 2000, podremos concluir que la tutela penal de la intimidad, ya no es simplemente tácita como en el Código Penal de 1980, sino expresa: Artículo 192. *Violación ilícita de comunicaciones*. Artículo 193. *Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas*. Artículo 194. *Divulgación y empleo de documentos reservados* Artículo 195. *Acceso abusivo a un sistema informático*. Artículo 196. *Violación ilícita de comunicaciones o correspondencia de carácter oficial*, y Artículo 197. *Utilización ilícita de equipos transmisores o receptores*.

El hecho punible en Colombia se divide en delitos y contravenciones (artículo 12 del C. P. Col.,), y éstas a su vez se dividen en ordinarias y especiales (artículo 12 del Código Nacional de Policía: Decretos 1355-2055 de 1970 y 522 de 1971, modificados parcialmente por la Ley 23 de 1991), atendiendo a la gravedad o levedad de la infracción y la sanción, el bien jurídico tutelado y la competencia de las autoridades. En tal virtud, siendo más graves las contravenciones especiales, se ha ubicado después de atribuir competencia a las autoridades administrativas locales y regionales, con funciones cuasi- jurisdiccionales [17] y asignarles el conocimiento de las contravenciones "que afectan la integridad personal", la intimidad o la "vida íntima o privada de una persona" (artículos.46 a 49), cuando sin facultad legal se la averigüe hechos o datos de la intimidad, se los graba con cualquier medio tecnológico de información o comunicación que llama "subrepticios", o los "divulga" u obtiene "provecho" de ese descubrimiento de información. Estas modalidades ilícitas se agravan si se hace a sabiendas, con conocimiento previo y sin justa causa.

3. LA INFORMATICA [18] JURIDICA DOCUMENTAL, 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 " el pleno ejercicio de sus derechos", según la Constitución Española de 1978 (artículo 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 (artículo 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 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 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 desfasado 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 artículo 15, constitucional colombiano, 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 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 post-industriales 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* [21], al analizar el derecho, la informática y la ciencia y al encontrar que el derecho va experimentar 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, etc, 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 [22], como parte de la informática jurídica.

Antes de la denominada época "post-industrial", 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 [23], Australia [24], 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 ius-penalista, 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 extra-penales, 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 [25] , 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.

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 tele-transmisión 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* [26] .

Con aquéllas finalidades, *Davara* [27] 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) [28]. 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* [29], 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.

En efecto, el profesor *Romeo Casabona* [30], 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* [31]--, clasifica a los delitos informáticos en cuatros grupos o categorías. Clasificaciones que sirven a la citada autora, a *Gutiérrez Francés* [32] y *Buenos Arus* [33], 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 artículo 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* [34], 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 artículo 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, artículos.12 y ss., principalmente.

Por su parte, *Carbonell y González*,[35] al estudiar el artículo 197.2 del Código Penal Español del 95, lo intitula: *Los delitos informáticos*, para seguidamente expresar que éste numeral 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 fenómeno informático en forma holística, pues el misma artículo 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* [36], 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 Código Penal Español 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 auto-desvirtuado, 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 artículo 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 artículos. 42 y 43 las enuncia 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.

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* [37] , 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*.

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 Código Penal Español de 1995, *Pérez Vallejo* [38], 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 litis, no impreso o no tradicional --teniendo en cuenta la nueva definición del artículo 26 del Código Penal Español 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 Capítulo I, "Del Descubrimiento y revelación de secretos, entra en una referencia directa a la informática" el artículo 197.2. No hace referencia a los delitos contra el honor, a pesar de citar el artículo 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" (artículo 238.4), es decir, las que enuncia el artículo239 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., artículo 248.2, contempla la "Estafa informática". En el Cap. IX, "De los daños", el artículo 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" Código Penal Español del 95). En la Sección 1, *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 Código Penal vigente nada nuevo destacable introduce a lo preceptuado en el anterior Código Penal Español., en los artículos. 534 bis a) a 534 ter.

4.1.4.2. Clasificaciones del delito informático en donde uno de los bienes jurídicos a proteger más importante es la *Intimidad*.

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 artículo 18.4, 20.1.d) y

105 CE, contra las injerencias de la informática.

El ius-penalista español *Morales Prats* [39], 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* (artículos. 197 a 204) del Código Penal Español del 95, y considera que la *privacy,* "libertad informática (faceta o perfil informático de la intimidad)", en el artículo 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 artículo 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 artículo197.2, en su redacción es sustancialmente mejor que la presentada en el proyecto de Código Penal de 1992 (artículo198.2) y del proyecto de Código Penal Español de 1994 (artículo188.2), 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 artículo 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 artículo 197.2. C.P.del 95, --dice el citado autor-- son: a) En el inciso primero, quedan tipificadas las acciones de apoderamiento, utilización o modificación 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 artículo 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 artículo 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 artículo 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 artículo197.5;

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 artículo 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 artículo 197.6 C.P, si conlleva la realización de los tipos anteriores (1 a 4 del artículo 197). Si además, se realiza en atención a la conducta prevista en el artículo 197.5, contra el *núcleo duro de la privacy*, se impone una *"pena hiperagravada de cuatro a siete años de prisión"*, como lo puntualiza el *Morales Prats* [40].

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 artículo 198 Código Penal Español, 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 artículo 22 del C.P.Esp.[41], sobre la prevalencia del carácter público que tenga el culpable; 2. Hacer referencia a cometer el hecho fuera de los casos previstos en la ley *"es meramente residual, pues se refiere a la falta de concurrencia de una causa de justificación"* [42] ; y, 3. Además de los *"defectos de coordinación sistemática* planteados por *Morales Prats"* [43], respecto del artículo 198 y los artículos. 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.

CITAS:

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

(2) Mi escrito intitulado: ***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. En: http://akane.udenar.edu.co/derechopublico

(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. También: en ***La tutela penal de la intimidad: privacy e informática***. Ed. Barcelona (Esp), 1984, pág. 33 DAVARA R. Miguel. *Manual de Derecho Informático.* Ed. Aranzadi, Pamplona (Esp.), 1997, pág. 285 y ss. CARBONELL M., J.C. y GONZALEZ CUSSAC., J.L. ***Delitos contra la Intimidad, el derecho a la propia imagen y la inviolabilidad de domicilio***. En: Comentarios al Código Penal de 1995. Vol. I., Ed. Tirant lo blanch, Valencia (Esp.), 1996, pág. 999 y ss. HEREDERO HIGUERAS, Manuel. ***La protección de los datos personales registrados en soportes informáticos*** .En: Actualidad Informática Aranzadi. A.I.A. Núm. 2, Enero, Ed. Aranzadi, Elcano (Navarra.), 1992. págs. 1 y ss.

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

(5) 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.

(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. Sent. T-486/1992, de 11 de Agosto. Sent. T-414-1992, de 16 de Junio). Textos completos en WWW.RDH.GOV.CO.

(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 (Nav.), 1996. pág. 309 y ss.

(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).

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

(16) VALLE MUÑIZ, José Manuel y MORALES PRATS, F.,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).

(16A) El Nuevo Código Penal Colombiano, que entrará a regir el 24 de Julio del 2001, establece en el Titulo III, DELITOS CONTRA LA LIBERTAD INDIVIDUAL Y OTRAS GARANTIAS, Capítulo VII, **De la violación a la intimidad, reserva e interceptación de comunicaciones**.

"Artículo 192. *Violación ilícita de comunicaciones*. El que ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida una comunicación privada dirigida a otra persona, o se entere indebidamente de su contenido, incurrirá en prisión de uno (1) a tres (3) años, siempre que la conducta no constituya delito sancionado con pena mayor.

Si el autor de la conducta revela el contenido de la comunicación, o la emplea en provecho propio o ajeno o con perjuicio de otro, la pena será prisión de dos (2) a cuatro (4) años.

Artículo 193. *Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas*. 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.

Artículo 194. *Divulgación y empleo de documentos reservados*. 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.

Artículo 195. *Acceso abusivo a un sistema informático*. 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.

Artículo 196. *Violación ilícita de comunicaciones o correspondencia de carácter oficial*. El que ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida comunicación o correspondencia de carácter oficial, incurrirá en prisión de tres (3) a seis (6) años.

La pena descrita en el inciso anterior se aumentará hasta en una tercera parte cuando la comunicación o la correspondencia esté destinada o remitida a la Rama Judicial o a los organismos de control o de seguridad del Estado.

Artículo 197. *Utilización ilícita de equipos transmisores o receptores*. El que con fines ilícitos

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

(17) Véanse, nuestros trabajos: ***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. En: http://akane.udenar.edu.co/derechopublico

(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: " 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).

(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.

(21) Citado en mi trabajo: ***La Constitución de 1991 y***... Ob. ut cit.pág. 51. En: http://akane.udenar.edu.co/derechopublico

(22) Véase, Mi escrito electrónico de ésta página de WEB, sobre LOS DATOS PERSONALES INFORMATIZADOS EN EL DERECHO FORÁNEO Y COLOMBIANO La informática Jurídica y los datos de carácter personal. Ficheros o Bases de Datos.. En: http://akane.udenar.edu.co/derechopublico

(23) 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.

(24) 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

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

(26) Ibídem pág. 304

(27) Ibídem pág. 288.

(28) 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”.

(29) 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.

(30) 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.

(31) PEREZ Valllejo. A. Ob cit., pág. 9.

(32) 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.

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

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

(35) 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

(36) 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.

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

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

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

(40) Id. pág. 321.

(41) SERRANO GOMEZ, Alfonso. ***Delitos contra la intimidad...*** pág. 235

(42) 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.

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

Actualización: Pasto, Abril 1 de 2008

INICIO