LA PROPIEDAD DE LOS DATOS Y LAS NUEVAS TECNOLOGÍAS: DEL "BIG BROTHER" AL CONTROL BIOMÉTRICO

DANIEL PEÑA VALENZUELA

INTRODUCCIÓN

La edad, el sexo, la raza, el origen familiar, la profesión, los documentos de identidad, los gustos, los hábitos, las costumbres, los intereses, las actividades preferidas, las preferencias de consumo son parte fundamental del individuo, lo diferencian de los otros, pertenecen en su mayor parte a su ámbito privado, son valores fundamentales de la personalidad[1].

Las modernas tecnologías de la información permiten recolectar, acceder, distribuir y manipular información sobre las personas utilizando bases electrónicas de datos, control del correo electrónico, técnicas de rastreo electrónico, uso de identificadores biométricos y bancos de ADN[2]. La información más íntima sobre un individuo puede ser conocida y utilizada por terceros, sin el consentimiento del sujeto, sin su autorización e incluso sin que el individuo sea consciente de la divulgación que ha realizado de dicha información. El sueño o pesadilla de Orwell se ha convertido en realidad[3].

Los datos son la materia prima de la sociedad de la información[4]. Se ha convertido, en consecuencia, en prioritario el análisis de la protección de los mismos por cuanto los ciudadanos son objeto de asedio por parte de la empresas comerciales y los gobiernos que usan todo tipo de estrategias para el recaudo de los datos personales. Sea mediante formularios en papel o electrónicos, los hábitos y costumbres son vigilados y controlados por técnicas de rastreo; los consumidores son a menudo objeto de publicidad personalizada gracias al previo conocimiento de los intereses y preferencias. Los particulares son también controlados en sus sitios de trabajo, el uso del correo electrónico, las videocámaras así como el monitorio a los sitios de internet visitados y tiempo de navegación a través de los mismos.

1. VÍCTOR PÉREZ VARGAS. "Los Valores de la Personalidad y el Derecho Civil de América Latina", ponencia presentada al Congreso Italo-latinoamericano sobre personas, ASSLA-Universidad Externado de Colombia, Bogotá, agosto de 1987.

2. MATT RIDLEY. *Genome: The Autobiography of a Species in 23 Chapters*, New York, Perennial, 2000.

3. GEORGE ORWELL (1903-1950) autor de 1984, obra cumbre sobre el control social de la cual surge la figura "big brothe" como ejemplo de la autoridad que controla a los individuos.

4. ADRIANA ZAPATA DE ARBELAEZ. "Perspectiva europea del comercio electrónico: Directiva 2000/31 CE del Parlamento Europeo y del Consejo", en *Comercio Elctronico. Memorias*, Bogotá, Universidad Externado de Colombia, 2000.

Los gobiernos por su parte, tienden a extender las posibilidades de vigilancia y control sobre las comunicaciones, en particular, es de actualidad el uso extendido de videocámaras, controles electrónicos de velocidad en las carreteras e intercepción al correo electrónico y a las comunicaciones telefónicas[5].

Dos ejemplos describen la importancia práctica del tema de la propiedad de los datos: (a) Ha sido ampliamente discutido por los tribunales colombianos el principio del *habeas data*[6] como forma de protección de datos personales, en especial, en el caso de la relación entre las bases de datos de las centrales de riesgo y los usuarios del sistema financiero. (b) En el caso del internet, la naturaleza técnica de la red ha creado unos nuevos paradigmas sociales, los *hackers*, individuos entre contestatarios y héroes que realizan proezas en internet al ingresar sin autorización a redes informáticas públicas y privadas[7].

En el presente artículo se va a analizar quien es el titular de los datos. La protección de las bases de datos mediante la propiedad intelectual, el derecho de la competencia y la protección de los secretos empresariales. La justificación y evolución histórica de la protección a la intimidad será descrita. Finamente algunos casos concretos en los que se ha expresado la problemática de la propiedad de los datos será revisada.

I. DATOS, PROPIEDAD Y BASES DE DATOS

A. ¿QUIÉN ES EL PROPIETARIO DE LOS DATOS?

Quien tiene la información tiene el poder. Este adagio popular utilizado en muchas situaciones cotidianas no es consecuente con el poco interés que la mayoría de ciudadanos y consumidores muestra en el valor e importancia que tiene la información personal. Con la disculpa de cualquier concurso o rifa o programa de actualización de datos, se entregan los datos personales sin restricción sobre su uso futuro. En Colombia, no existe activismo ciudadano ni de los consumidores para proteger su intimidad frente al gobierno o el comercio.

Los datos personales deben ser propiedad exclusiva del individuo por ser extensión de la persona misma. Este principio general y simple parece de fácil entendimiento y en principio no sería controvertible. Sin embargo, en la práctica, los datos personales son recolectados, almacenados, transformados, y manipulados por terceros que ejercen facultades similares a las que ejerce quien tiene el derecho de dominio respecto de un bien tangible.

Dos ejemplos ilustran este problema:

(a) Las bases de datos de las centrales de riesgo proveen a los operadores del sis-

5. Lawrence Lessig. *Code and other laws of cyberspace*, New York, Basic Books, 2000. El profesor Lessig plantea la teoría según la cual la regulación del ciberespacio, por influencia del gobierno y el comercio, se realiza a traves del 'Código' o sea, de la propia arquitectura de la red.

6. Artículo 15 Constitución Nacional.

7. Una vision especializada del tema de internet e intimidad se puede encontrar en Daniel Peña Valenzuela. "Privacidad y comercio electrónico", en *Revista Foro del Jurista*, n.º 22, Cámara de Comercio de Medellín, 2001.

tema financiero de la información sobre el crédito de un individuo, permiten determinar cuanto tiempo un deudor permaneció moroso, o si es un deudor que amerita tener crédito y en que condiciones y plazos, definen en consecuencia que información puede ser relevante para calcular el estado de las finanzas personales de un individuo. A menudo los datos son utilizados, sin el consentimiento expreso del sujeto, en otros casos, el consentimiento ha sido obtenido con mucha anterioridad al momento de celebración de crédito. No existe control del individuo respecto de sus datos, lo anterior justificado por un fin de interés general: la estabilidad del sistema financiero.

(b) Algunos portales de internet incluyen en sus políticas de intimidad la posibilidad de utilizar o vender o transferir los datos personales de usuarios que han recolectado mediante formularios electrónicos, por ejemplo, al momento en el que el usuario obtiene el derecho a usar una dirección de correo electrónico. El individuo entrega sus datos con el fin de obtener un servicio pero sus datos son luego cedidos a empresas que realizan propaganda directa mediante el envio de mensajes individuales a las casillas de correo electrónico sin previa autorización del usuario.

Las utilización de las nuevas tecnologías en consecuencia puede afectar seriamente los atributos esenciales de la propiedad de los datos personales, sea por interés económico, comercial o político. *El individuo solo es realmente propietario del dato en la medida que pueda controlar efectivamente su uso Realizar de manera eficiente la modificación de los datos de inexactitud del mismo. Evitar su transferencia a terceros sin previa autorización y poder conservar confidencial la información que considere pertinente.*

La intangibilidad del dato cuestiona la teoría general de los derechos reales en mayor medida que los derechos de propiedad intelectual pues estos como es bien sabido se registran ante autoridades administrativas, los datos no. No existen certificados de propiedad o títulos sobre los datos. La protección de los datos y de la intimidad se ha garantizado al establecerlo como un derecho fundamental con mecanismos judiciales específicos de protección.

La propiedad plena respecto del dato está fuertemente impactada por el derecho de la información. No siempre puede tenerse el control efectivo de una dato que a su vez tenga interés público La intimidad de un enfermo de Sida, por ejemplo, puede contraponerse a los imperativos de la salud pública.

B. LOS DATOS EN LAS BASES DE DATOS

Una lista de clientes o direcciones, un directorio telefónico, un índice de textos, una serie clasificada de precios de productos o servicios, pueden ser considerados como una base de datos[8]. Una base electrónica de datos es una compilación de información de cualquier especie que esta almacenada en un sistema electrónico de información[9].

Luego de múltiples discusiones sobre la manera eficaz de proteger a las bases de

8. DAVID BAINBRIDGE. *Software Copyright Law*, London, Butterworths, 1994.
9. Artículos 102 de ADPIC y 5.º del Tratado de la OMPI sobre Derecho de Autor del 20 de diciembre de 1996.

datos existe un consenso internacional en estas deben ser protegidas por el *derecho de autor*. Esta protección se refiere a la selección y configuración original de los datos[10]. La estructura y arquitectura de una base de datos es protegida[11] pero los datos que se incorporan en ella no son protegidos por la propiedad intelectual[12].

Tres situaciones jurídicas son fundamentales respecto de las bases de datos[13]:

(a) Si la información almacenada es de carácter personal, es importante determinar hasta que punto llega el derecho de la intimidad y la información confidencial sobre los datos es decir respecto del contenido de la base de datos,

(b) La responsabilidad de los "autores" –quienes ejercen el control– de las bases de datos por la veracidad de la información contenida en estas.

(c) La protección por el derecho de autor al contenido de las bases de datos en los siguientes eventos:

a. Cuando el contenido de la base de datos está constituida por obras preexistentes es necesaria la autorización previa y expresa del autor para dicha utilización;
b. La adaptación de las obras preexistentes por ser una transformación requiere de la autorización de los autores;
c. Cuando se accede a una base de datos por ejemplo mediante una pantalla de computador existe una comunicación pública que requiere una autorización;
d. Las copias impresas de obras preexistentes que estén en la base de datos constituye un acto de reproducción y debe ser autorizado, y
e. La puesta a disposición de las copias impresas constituye un acto de distribución y debe contar con el consentimiento del autor[14].

Como se puede ver la protección por una base de datos como una propiedad intelectual se limita a la forma de la base de datos. Sin embargo, ante el crecimiento en la inversión en las bases de datos, se ha discutido como el derecho de propiedad debe ser más amplio sobre todo cuando los datos no son protegidos legalmente. De esta discusión ha surgido el derecho de acceso a las bases de datos La pionera en tal innovación fue la Comunidad Europea, este proceso culminó en la Directiva 96/9 del 11 de marzo de 1996 de la Unión Europea por la cual se protegen las bases de datos no solamente mediante el derecho de autor sino también bajo un derecho *sui generis* de acceso o reutilización que está vinculado con la inversión económica que se haya hecho en la construcción de la base de datos[15].

La protección especial de la Unión Europea al acceso a las bases de datos está sujeta a las siguientes condiciones[16]:

10. Articulos 5.º literal b y 24 de la Ley 23 de 1982
11. Artículo 3.5 del Convenio de Berna.
12. Artículo 28 de la Decisión 351 de la Comunidad Andina.
13. Concepto de la Dirección Nacional del Derecho de Autor, Oficio 1193 del 25 de febrero de 2000.
14. Ibídem.
15. W. R. Cornish. *Intellectual Property*, London, Sweet & Maxwell, 2001.
16. Ibídem.

– Se aplica a las bases de datos independientemente de si también la base de datos está protegida por los derechos de autor;

– Se centra en el contenido de la base de datos y no en su organización o configuración. Su objetivo es evitar que el contenido pueda ser accedido o reutilizado;

– La base de datos debe ser el producto de una inversión sustancial, y

– El derecho dura 15 años desde que la base de datos haya sido terminada o haya sido puesta a disposición del público. En el evento que exista una nueva inversión el término inicial se renueva por otro período igual al primero.

Recientemente, se discutió también en los Estados Unidos la aplicación de las reglas de la ocupación ilegal de los bienes (*trespass*) a una empresa que había utilizado técnicas electrónicas con el fin de utilizar los datos de precios publicados en el *web site* de la empresa virtual de subastas *e-bay* con el objetivo de incluirlos en su propio sitio[17].

Lo anterior indica que el sistema europeo y el norteamericano de protección de las bases de datos converge hacia la protección de los datos en si mismos como información así como a la forma en que se realiza la selección y disposición para su utilización.

Sería interesente que Colombia estudiara la posibilidad de incluir la incorporación de un derecho sui generis de acceso como parte de la protección de las bases de datos por el derecho de autor.

La protección a los datos además se ratifica por la protección a las bases de datos por otras categorías jurídicas. En efecto, las bases de datos pueden ser mantenidas en confidencia y por lo tanto protegidas como *secreto empresarial*. Categoría de la propiedad industrial que protege cualquier información no divulgada que una persona natural o jurídica legítimamente posea, que pueda usarse en alguna actividad productiva, industrial o comercial, y que sea susceptible de transmitirse a un tercero, en la medida que dicha información sea:

– secreta, en el sentido que como conjunto o en la configuración y reunión precisa de sus componentes, no sea generalmente conocida ni fácilmente accesible por quienes se encuentran en los círculos que normalmente manejan la información respectiva;
– tenga un valor comercial por ser secreta, y
– haya sido objeto de medidas razonables tomadas por su legítimo poseedor para mantenerla secreta[18].

Las bases de datos, y los datos mismos, se pueden proteger, entonces, como información confidencial mediante el régimen de protección del secreto empresarial si se adoptan las medidas tecnológicas para que cumplan lo anteriores supuestos y mientras estos se mantengan[19]. Es importante que esa confidencialidad también sea un

17. Lawrence Lessig. *The Future of Ideas*, Nueva York, Random House, 2002.
18. Artículo 260 de la Decisión 486 de la Comunidad Andina.
19. Artículo 263 de la Decisión 486 de la Comunidad Andina.

derecho para quien quiera que determinados datos suyos no sean incluidos en las bases de datos o que exista el consentimiento previo para su recolección o uso.

Además de lo anterior, la información de las empresas hace parte de sus activos y su extracción indebida por terceros puede dar origen a actos de *competencia desleal*[20], también serían protegidos en la medida que su acceso o divulgación induzca a ruptura contractual, afecte el crédito mercantil de un competidor o desordene internamente a una empresa rival. En este evento, el acto de competencia desleal también podría ser un caso de enriquecimiento injusto.

Los diversos medios de protección de la propiedad de las bases de datos giran alrededor de dos aspectos fundamentales: (a) la selección y disposición de los datos y (b) los datos mismos. Además de los mecanismos del secreto empresarial y la competencia desleal, propios de la protección de la propiedad intelectual, los datos y la información se protegen por otras áreas del derecho como el derecho constitucional y el derecho comercial por el valor intrínseco y por el valor comercial de la información, respectivamente. Posiblemente, la convergencia de todas las formas de protección vistas en este capítulo constituyan una garantía completa para los propietarios de las bases de datos. Sin embargo, no debe olvidarse que subsiste la tensión entre los propietarios de las bases de datos y los propietarios de los datos.

II. EL DERECHO DE INTIMIDAD COMO JUSTIFICACIÓN DEL DERECHO DE PROPIEDAD SOBRE LOS DATOS PERSONALES

El artículo 12 de la Declaración Universal de los Derechos Humanos establece que "Nadie será objeto de injerencias arbitrarias 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 o ataques". La Constitución de 1991 protege la intimidad de los individuos como un derecho fundamental[21].

A. GENESIS DEL DERECHO DE LA INTIMIDAD

Grecia, Roma y el medioevo son citados como antecedentes de la noción de la protección de la intimidad de los individuos[22]. La diferencia entre lo público y lo privado, en cada etapa de la historia de la sociedad, ha justificado la existencia del poder político. Sin embargo, es en la época moderna[23] y por influencia de la concepción filosófica liberal[24], con acento individualista, que el

20. Artículo 16 de la Ley 256 de 1996.
21. Artículo 15 Constitución Nacional.
22. Federico Moeykens. "La proteccion de datos personales en el proyecto de Código Civil unificado con el Código de Comercio de la República Argentina", *REDI, Revista de Derecho Informático*, Buenos Aires, mayo de 1999.
23. Cfr. Luciano Parejo Alfonso, "Problemas actuales de los derechos fundamentales, el derecho fundamental a la intimidad", *Boletin Oficial del Estado*, Madrid, Universidad Carlos III, 1994; citado por John Gutiérrez Boada. *Los limites del derecho de la intimidad*, Bogotá, Universidad Externado de Colombia, 2000 p. 9.
24. Cfr. Pablo Lucas Murillo. "El derecho a la autodeterminación informativa", en *Temas clave de la Consitución española*, Tecnos, 1990 pp. 49 y ss.; citado por Gutiérrez Boada. Ob. cit.

derecho a la intimidad adquiere identidad y empieza a desarrollarse como un derecho ciudadano[25].

Con la invención de la imprenta se creó la posibilidad técnica de transmitir información escrita con el grado de abstracción y complejidad que oponía lo escrito a lo oral, permitiendo diseminar los conocimientos y la información de manera múltiple. El derecho de autor (*copyright*), apareció entonces, como la primera manifestación jurídica que impidió la publicación de cartas personales por cuanto su autor era quien tenía la propiedad sobre los mismas[26].

Con la aparición de los medios masivos de comunicación la inquietud de cómo mantener la intimidad se trasladó a la teoría tradicional de la responsabilidad civil[27] con el fin de que los ciudadanos estuvieran protegidos frente al poder de la prensa.

El primer planteamiento académico sobre el derecho de la privacidad lo hicieron los académicos SAMUEL D. WARREN y LOUIS BRANDEIS en su artículo de la *Harvard Law Review* sobre el *right to privacy* en 1840[28]. Esta doctrina inicial ha sido la fuente generatriz de protección en diversos casos.

La protección a la intimidad y a los datos personales han tenido dos etapas. La primera, estática, en la cual se plantearon los temas de la protección de los datos personales en cuanto a su acceso, rectificación y manipulación en las bases de datos y la segunda, dinámica, que aparece simultáneamente con la masificación en el uso de internet. Este nuevo medio ha obligado a organizaciones como la *Federal Trade Comission* y a la Comisión Europea a replantear los fundamentos de la protección a la intimidad en particular en relación con las transacciones electrónicas entre empresas y consumidores.

Tres de los temas de mayor discusión internacional, aún no resueltos, sobre la protección a la intimidad se refieren a:

– Derecho a practicar exámenes de laboratorio al momento de nacer a bebes descendientes de enfermos con Sida con el fin de determinar si tienen tal enfermedad y deben recibir una droga especial que previene o aplaza los efectos devastadores de la patología mencionada.

– La posibilidad de revelar los antecedentes judiciales-penales de un individuo que convive en una comunidad luego de haber cumplido una sanción penal. Lo anterior teniendo en cuenta que estadísticamente estos antecedentes pueden repetirse en el caso de delitos sexuales y con el fin de evitar que si el individuo reincide pueda afectar a miembros de la comunidad (casos de violadores a menores).

25. HUMBERTO QUIROGA LAVIE. Derecho a la intimidad y objecion de conciencia, en *Colección Temas de Derecho Público*, Bogota, Universidad Externado de Colombia, p. 54.

26. MARIE CLAUDE PREMONT. *Donnees personnelles et secret de la vie privee apprche nord americaine en nouvelles technologies et propriete*, Paris, LITEC, 1991, pp. 74 y ss.

27. Ibídem.

28. AMITAI ETZIONI. *The Limits Of Privacy*, New York, Basic Books, 2000.

ETZIONI examina la historia del derecho de la privacidad en los Estados Unidos en tres etapas*: In examining the arguments that were used to formulate the legal doctrines that support privacy in American law, I discuss three stages of development: pre-1890 (utilizing principles derived from property rights to protect privacy); 1890 to 1965 (generally considered the era during which a right to privacy was developed, largely as a part of tort law) and post-1965 (a period that has seen a major expansion of the right to privacy, particularly with regard to its constitutional basis).*

– La posibilidad de revelar la historia clínica de pacientes a terceros, por ejemplo, empresas aseguradores con fines, por ende, diferentes a los terapéuticos[29].

Ejemplos de la creciente tendencia a legislar sobre privacidad en la era electrónica son: la ley de protección de los datos personales y de los documentos electrónicos de Canadá –Personal Information and Electronic Documents Act, 2000–[30], la ley de protección de datos personales del Reino Unido –Data Protection Act, 1998–[31] y la ley de protección de la privacidad de los infantes en las actividades en línea de los Estados Unidos[32].

Lo anterior refleja que el tema de la protección de datos hace parte de la agenda de la globalización y dejar de lado su regulación en Colombia puede afectar la competitividad del país y sus empresas. Lo anterior sin embargo debe ser coherente con las garantías constitucionales al derecho fundamental de intimidad. Los datos personales de los ciudadanos deben ser protegidos por el estado como asunto de interés nacional y su excesiva o falta de protección podrán ser objeto en el próximo futuro de litigios internacionales por ejemplo bajo las reglas del comercio internacional como los paneles de resolución de conflictos de la Organización Mundial de Comercio.

B. EL DERECHO A LA INTIMIDAD EN COLOMBIA

La primera referencia al derecho a la intimidad en Colombia como derecho constitucional fundamental aparece en el proyecto de acto reformatorio de la Constitución de 1886[33] que propuso el Gobierno del presidente VIRGILIO BARCO, dentro de los cambios propuestos al capítulo de derechos fundamentales. En ese momento se planteó un régimen general de garantía al derecho de la intimidad personal y familiar. Además se establecía que la ley reglamentaría el uso de la informática y de otros avances tecnológicos para garantizar la intimidad personal y familiar y el pleno ejercicio de otros derechos.

La Asamblea Constituyente se limitó a establecer el derecho a la intimidad personal y familiar en el artículo 15 de la Constitucion de 1991[34]. La información que se haya recolectado en bancos de datos y en archivos de entidades públicas y privadas pueden ser conocidas, actualizadas y rectificadas a petición de los ciudadanos[35].

El desarrollo que ha tenido el tema de la intimidad y el uso ciudadano de los medios electrónicos ha sido principalmente en el campo del *habeas data* o sea en la posibilidad en cabeza de personas naturales o ju-

29. ETZIONI. *The Limits Of Privacy*, cit.

30. ELIZABETH MCNAUGHTON y ELYSSA WORTSMAN. *Privacy*, a special edition of the Blakes Report on Intellectual Property, Quebéc, abril-mayo, 2000.

31. *Data Protection Briefing* de Paisner & Co., Londres, 2000.

32. Children On line Privacy Protection Act, 2000.

33. La Constitucion de 1886 no reconocía expresamente el derecho a la intimidad, sin embargo, existían principios constitucionales que permitían, interpretados en conjunto, construir la teoría del derecho de la intimidad: la prohibición de perturbar a la persona o a su familia, la inviolabilidad del domicilio y la correspondencia y la protección de la honra de las personas.

34. MANUEL JOSÉ CEPEDA. *La constituyente por dentro*, Consejería para el Desarrollo de la Constitución-Presidencia de la República, 1993, pp. 41 y ss.

35. MANUEL JOSÉ CEPEDA. *Los derechos fundamentales en la Constitución de 1991*, Bogotá, Temis-Consejeria para el Desarrollo de la Constitución-Presidencia de la República, 1991, pp. 50 y ss.

rídicas de rectificar datos erróneos o no actualizados consignados en las bases de datos de carácter comercial o criminal[36].

No ha sido explorado, sin embargo, el alcance del texto constitucional frente a prácticas ya frecuentes en Colombia como por ejemplo la recolección, y en algunos casos exportación, de datos personales por parte de proprietarios de sitios de internet que tienen alcance en el territorio colombiano. Tampoco es evidente el valor jurídico y sanciones respecto del control y monitoreo que realizan empleadores del correo electrónico de sus empleados.

Actualmente se está discutiendo en el congreso un proyecto de ley estatutaria para reglamentar el derecho fundamental a la intimidad[37]. Desafortunadamente, dado el calendario electoral en el presente año es posible prever que este asunto no será prioritario en la agenda legislativa. Si lo anterior se confirma nuestras empresas perderían otro factor importante de competitividad internacional. No es entendible tampoco que la protección de los datos haya sido dejada de lado de los temas prioritarios de la Comunidad Andina.

C. ¿QUIÉN AMENAZA LA INTIMIDAD?

La amenaza a la intimidad de los individuos proviene de diversas fuentes:

1. *Las empresas y comerciantes* cuyo interés es obtener el mayor lucro posible en sus negocios y que, de acuerdo con las técnicas de mercadeo, aprovechado cualquier posibilidad para obtener la mayor información posible de los consumidores.

Existen mecanismos que permiten efectuar seguimientos de usuarios y creación de perfiles, y que pueden tener ciertos aspectos preocupantes. Algunos ejemplos son:

(a) *Web Bugs*. Estos son gráficos utilizados en páginas web o mensajes de correo en HTML[38], y que sirven para monitorear a quien visita dichas páginas o lee dicho correo.

Los web bugs no pueden ser "bloqueados", por los usuarios, ya que al tratarse de imágenes, es imposible generar un filtro, para determinar cuales son imágenes propias del sitio web y cuales son web bugs. Una forma de estos bugs son las cookies o archivos electrónicos que se depositan en el disco duro de los navegantes y que permite rastrear los hábitos y costumbres de los usuarios.

(b) *Software de Servicio al Cliente*. En esta categoría podemos encontrar variados programas, los más conocidos Human Click y Live Person.

En la página web se insertan unas líneas de código java-script. Luego, en el centro de atención al cliente, se instala el software. Así, cada operador, puede "vigilar" en que momento ingresa alguien al sitio web. Se puede ver a los usuarios navegando en su sitio, verlos recorrer cada sección y página del sitio, saber cuanto tiempo utilizan en cada una, y además, ofrecerles en pantalla ayuda en tiempo real.

36. Las principales sentencias de la Corte Constitucional respecto del tema de las bases de datos y el habeas data son: sentencias C-114 del 15 de marzo de 1993, T-22 del 29 de enero de 1993, SU-082 del 1.º de marzo de 1995, SU-89 del 1.º de marzo de 1995, T-462 de 1997, T-527 de 2000.

37. Proyecto de Ley Estatutaria 52 de 2000 del Senado, en *Gaceta del Congreso*, n.º 317, Bogotá, 10 de agosto de 2000.

38. Hyper Text Mark Up language, lenguaje de programación de páginas de internet.

Así, si el usuario lo solicita, se abre una ventana de Chat y se responden las dudas que el tenga.

LivePerson, por ejemplo, es un software muy avanzado y tiene por objeto ayudar la administración de servicio al cliente. Su más interesante característica es la administración de base de datos de clientes. Permite generar perfiles de los usuarios, crear prospectos de venta, generar campañas de e-mail y marketing.

(c) *Video cámaras*, que permiten actualmente procesar archivos electrónicos que contienen imágenes digitalizadas y que pueden ser almacenados en bases de datos.

Los empresarios conocen el valor agregado que tiene saber los hábitos de los consumidores y su importancia como herramienta para el mercadeo directo de bienes y servicios, especiamente en un contexto marcado por una fuerte competencia en un ámbito global y los gobiernos –y en especial los organismos de seguridad de los Estados– cuya función es defender los intereses colectivos a través de estrategias de control a los ciudadanos, generalmente con el respaldo de competencias atribuidas por la ley.

Después de los sucesos del 11 de septiembre la tendencia en el mundo, en particular en los Estados Unidos es la autorización sin límite alguno a los organismos de seguridad para rastrear e interceptar las comunicaciones. El *Patriot Act de 2001* permite la vigilancia de los correos electrónicos que pasen por plataformas ubicadas en los Estados Unidos. En Colombia, la interceptación y registro de las comunicaciones, incluído el correo electrónico solo puede darse mediante orden judicial, por cuanto son comunicaciones privadas para los efectos del artículo 192 del Código Penal. Sin embargo. muchos de los ciudadanos colombianos que tengan cuentas de correo electrónico con servidores de correo ubicados en Estados Unidos pueden estar sujetos al *Patriot Act.*

(1) Los *Hackers*, individuos con una alta capacidad y conocimiento sobre los sistemas y la informática que gracias a sus habilidades, malicia y en algunos casos, mala fe, acceden a los archivos electrónicos, a los servidores y en general, a los sistemas informáticos de empresas o individuos. Los *hackers* violan los sistemas informáticos de seguridad con el fin de difundir virus[39], alterar alguna informacion o simplemente lograr el acceso sin autorización[40].

Los *Hackers* son un símbolo de la idea libertaria de internet, de la oposición a la creciente influencia que tienen las grandes empresas multinacionales y los gobiernos respecto de la infraestructura y los contenidos en la red.

El costo económico de las intrusiones de los *hackers* es muy alto. MCI perdió cerca de cincuenta millones de dólares cuando, por ejemplo, una intrusión ilegal accedió a cincuenta mil números de tarjetas de crédito[41] y CitiBank perdió diez millones de dólares cuando los controles de su red fueron violados por un grupo criminal en Rusia[42].

39. GROSSMAN. Lev. "Attack Of The Love Bug", *revista Time*, 15 de mayo de 2000 y "E-bug Shows Up Manilas Legal Holes", *Financial Times*, 10 de mayo de 2000, Londres, p. 8.

40. Sobre la sociologia de los *hackers* cfr. suplemento de la revista *El Viejo Topo*, n.º 72, Madrid, febrero de 1994.

41. DAVID GRIPMAN. "The Doors Are Locked But The Thieves And Vandals Are Still Getting In. A Proposal In Tort To Alleviate Corporate Americas Cybercrime Problem", *John Marshall Journal of Computer Law & Information*, n.º 16, 1997, pp. 169 y 170.

Internet ha exacerbado la actividad de los *hackers* y ha obligado la creación de mecanismos de seguridad para luchar contra las intrusiones ilegales[43]. Incluso organizaciones internacionales como la OCDE (Organización Económica de los Países Desarrollados) ha propuesto que exista un regulador central que estudie medidas de prevención y quizás establecer sanciones por irrupciones a las redes informáticas con repercusiones globales.

Bajo iniciativa de la Organización Mundial de la Propiedad Industrial (OMPI) en el Tratado WCT o tratado de internet sobre Derecho de Autor[44], recientemente aprobado en Colombia y que ha sido incluído en el nuevo Código Penal, establece como hecho punible el acceso no autorizado a redes de computadoras y la violación a los mecanismos de protección de los derechos patrimoniales de autor[45].

Todo lo anterior sugiere que la el derecho constitucional de la intimidad se ha convertido en la base del derecho de protección a los datos en particular respecto de su divulgación y manipulación por terceros diferentes al propietario de los mismos.

III. PROBLEMAS RECIENTES DE LA PROTECCIÓN DE LOS DATOS

A. PROTECCIÓN A LA PRIVACIDAD DE LA INFORMACIÓN INFANTIL EN LÍNEA

Otro instrumento interesante de regulación estatal al tema de la intimidad es el de una ley federal en los Estados Unidos[46]

42. MARC GOODMAN. "Why The Police Don't Care About Computer Crime", *Harvard Journal of Law and Technology*, n.º 10, (1997) pp. 465 y 472.

43. Un completo resumen de los mecanismos técnicos utilizados por los hackers así como los mecanismos de seguridad se puede consultar en el artículo de MICHEL LEE et ál. "Electronic Commerce Hackers and the Search for legitimacy: a regulatory Proposal", trabajo ganador del Premio de 1998 de la *Berkeley Technology Law Journal*.

44. El artículo 11 del Tratado WCT establece:

Artículo 11.- *Obligaciones relativas a las medidas tecnológicas*. Las Partes Contratantes proporcionarán protección jurídica adecuada y recursos jurídicos efectivos contra la acción de eludir las medidas tecnológicas efectivas que sean utilizadas por los autores en relación con el ejercicio de sus derechos en virtud del presente Tratado o del Convenido de Berna y que, respecto de sus obras, restrinjan actos que no estén autorizados por los autores concernidos o permitidos por la ley.

En publicación OMPI n.º 226(S), Ginebra, septiembre de 1997.

45. El artículo 272 de la Ley 599 de 2000 (nuevo Código Penal) establece:

Violación a los mecanismos de protección de los derechos patrimoniales de autor y otras defraudaciones:

Incurrirá en multa quien:

1. Supere o eluda las medidas tecnológicas adoptadas para restringir los usos no autorizados.

2. Suprima o altere la información esencial para la gestión electrónica de derechos, o importe, distribuya o comunique ejemplares con la información suprimida o alterada.

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

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

46. The Childrens Online Privacy Protection Act vigente a partir del 21 de abril de 2000.

que obliga a los propietarios de los sitios de internet con propósitos comerciales que recolectan información personal de niños menores de trece años, a obtener el consentimiento de los padres de familia.

La ley establece que los sitios deben proveer a los padres de una notificación sobre sus prácticas sobre la información, obtener un consentimiento verificable sobre la recolección de información personal sobre los niños, otorgar a los padres la libre escogencia acerca de si la información del niño puede ser divulgada a terceras personas, permitir a los padres el acceso a la información recolectada sobre el niño y su corrección si es necesaria, y requerir a los niños únicamente la información necesaria para la actividad específica del sitios de internet[47].

En Colombia, la Ley 679 de 2001 se refiere por primera vez a la violación de los derechos de los menores mediante la utilización de la red global pero su ámbito de aplicación se refiere específicamente a la pornografía y el tráfico sexual y no sería suficiente para proteger la intimidad de los niños colombianos[48].

b. la protección de la intimidad de los datos personales como fuente de conflicto entre la unión europea y los estados unidos

La Unión Europea, desde el final de la segunda guerra mundial, han establecido regulaciones que tienden a garantizar la intimidad de sus ciudadanos. Las compañías europeas se han visto obligadas a evitar la utilización de los registros de datos personales para cualquier fin diferente al que originalmente habían sido recolectados[49].

Esta regulación surge como una reacción de pueblos y gobernantes europeos a los excesos cometidos por los aparatos de vigilancia empleados por el Tercer Reich. Los estados europeos, en particular Alemania, Francia e Inglaterra pusieron en funcionamiento entidades administrativas encargadas de vigilar y defender la privacidad de sus ciudadanos.

La masificación del computador personal y de la información electrónica en los años ochenta coincidió históricamente con el relanzamiento de la Comunidad Económica Europea y el proceso de establecimiento de la Unión Europea. Por consiguiente, el tema de la privacidad ha sido central en la construcción de una legislación uniforme y armónica en los Países Miembros. En 1995, la Directiva Europea de Protección de datos fue finalmente aprobada[50].

Las disposiciones principales de la Directiva establecen que: los datos personales no pueden ser divulgados sin el permiso expreso de los individuos, el derecho ciudadano a revisar cualquier información recolectada y corregirla si existe alguna inexactitud, prohibe la transmisión de datos desde el territorio de la Unión Europea hacia países que no brinden un nivel adecuado de protección.

47. Comunicado de Prensa de la Federal Trade Commission de los Estados Unidos del 20 de abril de 2000 en [www.ftc.gov].

48. Ley 679 de 2001 (3 de agosto), en *Diario Oficial* n.º 44.509 del 4 de agosto de 2001, por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía.

49. Yves Poullet. "Le Fondement Du Droit A La Protection Des Donnees Nominatives: Proprietes Ou Libertes", en *Nouvelles Technologies et Propriete*, Paris, litec, 1991, p. 75.

50. Directiva 95/46/CE sobre la protección de los individuos en relación al procesamiento de datos personales y sobre la libre circulación de esos datos, del 24 de octubre de 1995.

Los Estados Unidos, de otra parte, han construido la teoría del *right to privacy* a través de decisiones jurisprudenciales basadas en la cuarta enmienda constitucional[51]. La noción de *privacy* se ha adaptado a los retos de cada época pero sin que exista una legislación específica sobre el tema. Recientemente[52] la Comisión Federal de Comercio profirió una recomendación al gobierno respecto de la necesidad de una regulación legal que proteja la privacidad de los consumidores en línea. Esta regulación pretende complementar los esquemas de autoregulación existentes y prevalecer frente a las diversas regulaciones estatales sobre el tema.

En marzo de 2000, fue celebrado un acuerdo entre los Estados Unidos y la Unión Europea cuyo componente básico es el principio de *Safe Harbor.* Este principio exime a las compañías norteamericanas de ser demandadas por infracción a la privacidad, a iniciativa de los ciudadanos europeos, si han comunicado al Departamento de Comercio o a una autoridad de protección de datos europea que cumplieron con las regulaciones de la Directiva sobre protección de datos. En el evento que no sea veraz la declaración, las compañías pueden ser acusadas de *deceptive business practices (prácticas comerciales engañosas)* por parte de la Comisión Federal de Comercio y las autoridades judiciales norteamericanas.

Las iniciativas de la Unión Europea, han generado la reacción de algunos países en desarrollo que han optado por establecer *estándares* de protección que permitan continuar con un intercambio de datos entre las empresas, fenómeno que se podría describir como mecanismos de s*afe harbor de facto*[53]. Hasta el momento ha habido una gran aceptación de estas políticas por parte de los empresarios norteamericanos, es decir, los estándares europeos están siendo adoptados de manera predominante. En todo caso, es evidente que la noción de protección a la intimidad está enraizada en las costumbres sociales y las visiones diferentes de los países latinos, anglosajones y orientales y eslavos marcan diferencia en la regulación legal.

c. protección de los datos en las politicas de intimidad en los sitios de internet

La recolección de datos personales de los navegantes en internet es una de las actividades usuales llevadas a cabo por los propietarios de sitios y portales. La regulación sobre las condiciones, y autorización previa para la recolección de datos puede ser legal o contractual.

En algunos países, las condiciones a las que está sujeta la recolección de datos así como su tratamiento y manejo están definidos en leyes específicas al tema[54]. El control, regulación y sanciones son determinados por comisiones especiales, conformadas por funcionarios públicos o ciudadanos cumpliendo funciones ad-hoc.

51. La decisión Loving v. Virginia (1967) terminó con la penalización del matrimonio interracial; Eisenstadt v. Baird (1972) amparó la distribución de contraceptivos entre personas no casadas; Roe v. Wade (1973) amplió la protección del derecho de la intimidad a la decisión de la mujer embarazada de proseguir o interrumpir su embarazo.

52. El 22 de mayo de 2000.

53. "New Privacy Laws Have Eye On E.U. Data Privacy Directive", en *World Internet Law Report*, vol. 1, Issue 14, BNA, Londres, noviembre de 2000.

54. JEAN FRAYSSINET. *Informatique, Fichiers Et Libertés*, Paris, LITEC, 1992, en particular los capítulos II, III, IV y V.

Las leyes específicas sobre intimidad y manejo de datos se complementan con las políticas incluídas por los particulares en los sitios de internet, las cuales suelen publicarse en línea como parte del contenido del sitio. La inclusión de las politicas de privacidad ha sido usual desde el momento en el que la Comisión Federal de Comercio realizó recomendaciones en 1998 sobre la protección de los consumidores en los Estados Unidos. El análisis de las políticas de privacidad debe incluir la determinación de su naturaleza, si son disposiciones con efecto de eximir la responsabilidad, si tienen efecto legal y cuáles son sus límites frente al derecho positivo, principalmente, frente a la Constitución.

En Colombia, la Ley 527 de 1999[55] al validar la negociación electrónica y revestir a los mensajes de datos de valor probatorio permite afirmar que el colocar en línea un texto, en este caso la política de protección de datos e intimidad, que puede ser accedido y aceptado a través de un clic o el envio de un mensaje de datos tiene un valor probatorio equivalente a si se hubiera puesto en conocimiento del consumidor a través de un texto escrito en medios tradicionales.

Los dueños de sitios de internet, portales y centros comerciales virtuales que tienen alcance al territorio colombiano[56], usualmente con inversión de capital extranjero, suelen incluir la cláusula compromisoria mediante la cual cualquier conflicto con los usuarios derivado de la violación de las políticas de privacidad o respecto de la propiedad de los datos personales deberá ser definida bajo las leyes diferentes a las de Colombia y adjudicada por un juez o tribunal de arbitramento extranjero[57].

La eficacia jurídica de esas cláusulas podría ser cuestionada frente al derecho fundamental a la intimidad que puede ser fundamento de posibles acciones de tutela presentadas por ciudadanos colombianos. También es discutible si la aceptación de los términos y condiciones de uso de los sitios de internet y las políticas de protección a la intimidad son contratos de adhesión y las cláusulas autorizando la manipulación y tráfico entre fronteras de los datos son abusivas y, en consecuencia sujetas a nulidad o inexistentes.

d. la corte constitucional y el habeas data en los sitios de internet

La Corte Constitucional de Colombia declaró ajustada a la Constitución[58]. la norma que ordena a todas las páginas web y los sitios de internet de origen colombiano que operan en el internet y cuya actividad económica sea de carácter comercial, financiera o de prestación de servicios, *a inscribirse en el registro mercantil y a suministrar a la Dirección de Impuestos y Aduanas Nacionales-DIAN,* la información de transacciones económicas en los términos que esta entidad lo requiera.

55. Ley 527 del 18 de agosto de 1999 por medio de la cual se define y reglamenta el acceso y uso de lso mensajes de datos del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposciones, en particular, los artículos 2.º, 6.º, 7.º, 8.º, 9.º, 10.º, *Diario Oficial*, n.º 43.673, Bogotá, 21 de agosto de 1999.

56. Como ejemplos se pueden consultar la Privacy Policies de Amazon [www.amazon.com]; yahoo [www.yahoo.com] y Terra [www.terra.com].

57. Cfr. Ley 315 del 12 de septiembre de 1996, en *Revista Legislación Económica*, n.º 1056, Bogotá, octubre.

58. Corte Constitucional, Sentencia C-1147 del 31 de octubre de 2001.

Sin embargo, la Corte impuso a las autoridades tributarias colombianas ciertas condiciones a la hora de aplicar esta disposición:

- deberán respetar el principio de la finalidad,
- el principio de la relevancia
- el derecho a la privacidad y
- el *habeas data* de los agentes involucrados.

El caso se originó por una demanda que presentó un ciudadano que consideraba que:

- Tal disposición vulneraba la Constitución pues imponía en una ley tributaria (Ley 633 de 2000) una obligación propia de la ley comercial (el registro mercantil).
- Entregaba a la autoridad tributaria un poder excesivo.
- Era vaga en cuanto a su jurisdicción pues no se sabía a ciencia cierta cuáles páginas eran de origen colombiano.

En cuanto al primer punto, la Corte desestimó la demanda pues consideró que el aparte de la norma que imponía una obligación comercial era compatible con una ley tributaria pues al fin y al cabo se trataba de dos obligaciones que recaían sobre el mismo sujeto y facilitaban al Estado su función de control.

En cuanto al segundo punto, la Corte condicionó las facultades a de la administración tributaria a que en la solicitud de información se respeten los siguientes derechos:

– El derecho a la intimidad de quienes realicen transacciones electrónicas.

– El principio de relevancia, el cual supone, en cada caso concreto, que sólo puede requerirse y revelarse la información que esté relacionada con las funciones legalmente atribuidas a la entidad que la solicita.

– El principio de finalidad de modo que la información requerida y revelada sea:

(i) estrictamente necesaria para cumplir los fines de la administración en ese caso concreto, y

(ii) sólo sea utilizada para los fines autorizados por la ley que, en el presente caso, tienen que ver con la inspección, recaudo, determinación, discusión y administración de asuntos tributarios en los términos específicos que señalan las disposiciones legales para cada tributo en particular.

Ahora bien: la Corte aclaró que es posible que la administración de impuestos requiera en casos concretos y excepcionales, de información más detallada acerca de las transacciones que se realizan por internet. En estos eventos el ejercicio legítimo de las facultades de investigación que se le conceden a la DIAN exige justificar la pertinencia de tales datos, de manera tal que se demuestre la relación directa entre lo que se solicita y la materia que es objeto de estudio, en aplicación del principio de relevancia. Además, en estas circunstancias tendrán que respetarse los criterios que velan por la adecuada conservación y destinación de la información recaudada.

La primera incursión de la Corte en los temas del ciberespacio y la intimidad fue afortunada en nuestra opinión pues establece criterios de interpretación que pueden ser útiles para los empresarios de la red. Sin embargo, los casos concretos que se lleven bajo el mecanismo de la tutela pueden ser aún más constructivos.

e. la intimidad del correo electrónico de los empleados

La protección a la intimidad en las comunicaciones electrónicas y en particular, del correo electrónico utilizado por los empleados de una compañía en su trabajo es otro asunto debatido. Es frecuente que las compañías manejen su comunicaciones internas y externas mediante correo electrónico. El uso de esa herramienta puede servir para que un empleado realice actos ilegales por ejemplo, para obtener contenidos que infrinjan derechos de propiedad intelectual, realizar actividades contrarias al orden público, a las costumbres sociales, divulgar datos confidenciales de los clientes de la empresa, permitir acceso a secretos empresariales en la red o para realizar actuaciones y actividades representando de manera ilegítima a la compañía[59].

Los empleadores han comenzado a establecer políticas de intimidad[60] en las cuales se determinen las formas de uso del correo electrónico y en algunos casos mecanismos de vigilancia, control y fiscalización como por ejemplo la generación automática de archivos duplicados a manera de *back up*, para prevenir o sancionar los posibles abusos[61]. Estas políticas pueden hacer parte de los reglamentos internos de trabajo o ser incluidos en los contratos laborales.

Un caso inglés recientemente reportado en la prensa colombiana[62] ilustra claramente lo anterior. En efecto, el abogado británico Bradley Chait recibió un correo electrónico en el que su novia le felicitaba por sus proezas sexuales de la noche anterior y él reenvió el mensaje a seis de sus amigos. Ellos a su vez lo reenviaron a otras personas y el mensaje, que contenía además los nombres completos e indicación de los lugares de trabajo de la pareja en cuestión, terminó siendo de dominio público en todo el mundo. Los empleadores del famoso abogado confirmaron públicamente que abrieron un expediente para analizar posibles sanciones por violación de las normas laborales de la oficina de abogados que prohibían a sus empleados el envío o la recepción de material no relacionado con el trabajo.

Dada la rigidez del derecho laboral respecto a la necesidad de que las causales de terminación de los contratos de trabajo estén expresamente contempladas, sería conveniente que el Código Sustantivo del Trabajo sea reformado para incluir al abuso por el personal de las formas de comunicación y del uso de internet como causal expresa de terminación

Actualmente, existen varias normas del código sustantivo del trabajo que pueden aplicarse para regular la tensión de los patrones y empleados respecto de la intimidad. Es una obligación especial del patrono guardar absoluto respeto a la dignidad personal del trabajador, dentro de la cual se debe garantizar la intimidad[63]. En el

59. "Ahí viene el jefe" *Revista Puntocom*, Miami, octubre de 2000, p. 106.

60. Amy Rogers. "You Got Mail But Your Employer Does Too: Electronic Communication And Privacy In The 21st Century Workplace", *Journal of Technology Law & Policy*, vol. 5, Miami, Florida University, 2000, p. 25.

61. Rod Dixon. "With Nowhere To Hide: Workers Are Scrambling For Privacy In The Digital Age", *Journal of Technology Law & Policy*, vol. 4, Miami, Florida University, 1999, p. 34.

62. Periódico *Portafolio*, Bogotá, 20 diciembre de 2000, p. 13.

63. Artículo 57 (5) cst.

mismo sentido, esta prohibido a los patronos ejecutar o autorizar cualquier acto que vulnere o restrinja los derechos de los trabajadores o que ofenda sus dignidad, la interceptación de las comunicaciones podría ser considerada como un acto violatorio de la dignidad de los trabajadores.

Desde la perspectiva de los patronos, el uso indebido del correo electrónico o de internet puede ser considerado como una violación a la prohibición de los trabajadores de usar los útiles o herramientas suministradas por el patrono en objetos distintos del trabajo contratado[64]. Tampoco puede el trabajador comunicar por cualquier medio, incluyendo el correo electrónico, a terceros información confidencial o reservada del patrono o de la empresa[65].

Algunos empleadores han establecido filtros de información en los servidores para evitar el acceso a determinados sitios durante horas laborales[66]. Los mecanismos de vigilancia pueden en muchos casos llegar hasta el punto de controlar los sitios de internet a los que puede acceder un empleado o la recepción de correo electrónico privado a través de las redes del empleador, esta última medida, por ejemplo, para prevenir la difusión de virus. Muchas de estas medidas pueden ser cuestionadas desde la óptica del derecho de la intimidad[67]. En Colombia se podría generar la nulidad o ineficacia de las respectivas cláusulas contractuales, por ejemplo, en el marco de una acción de tutela basado en el derecho fundamental a la intimidad que podría ser considerado como no renunciable.

f. Caducidad de los datos en Colombia: derecho de la vivienda digna frente al derecho a la información

A partir de la sentencia SU-082 de la Corte Constitucional, se fijaron algunos parámetros de razonabilidad sobre la permanencia de los datos en los archivos electrónicos de las entidades para permitir que la anterior conducta del deudor no pueda ser mantenida a perpetuidad en detrimento de sus intereses y también preservar el derecho de las entidades financieras a estar informadas sobre los antecedentes crediticios de sus actuales o potenciales clientes con el fin de calcular los riegos al otorgar nuevos créditos.

En la mencionada sentencia se fijaron unos límites de la caducidad del dato, a la espera de una reglamentación del legislador al artículo 15 constitucional. Según la mencionada sentencia, sería irrazonable la conservación, uso y divulgación informática del dato, si no se tuviera en cuenta la ocurrencia de todos los siguientes hechos: (a) un pago voluntario de la obligación; (b) el transcurso de un término de dos (2) años a partir de dicho pago, excepto en el caso en que la mora haya sido inferior a un (1) años, en cuyo caso el término de caducidad será igual al doble de la misma mora; y (c) que durante el término antes

64. Artículo 60 (8) CST.
65. Artículos 58 (2) y 63 (8) CST.
66. Francis Cairncross. "Talking To Each Other", *The Economist*, Londres, Survey sobre e-management, 11 de noviembre de 2000.
67. María Helena Barrera y Jason Montague. "Correspondencia digital: recreando privacidad en el ciberespacio", *REDI, Revista Electrónica de Derecho Informático*, Madrid, junio de 1999.

mencionado, no se hayan reportado nuevos incumplimientos del mismo deudor, en relación con otras obligaciones.

Recientemente se ha discutido en Colombia, el conflicto entre el derecho a la vivienda digna y al de información contenido en el artículo 15 de la Constitución Nacional[68]. Las instituciones de crédito tienen derecho a conocer la solvencia económica de los usuarios de los servicios financieros por cuanto tienen a su cargo el ahorro nacional, es decir un tema de interés general. Los usuarios por su parte tienen derecho al *habeas data*, es decir, tienen derecho a conocer, actualizar y rectificar la información sobre estos que posean los propietarios de las bases de datos.

La ley[69] estableció que las personas que dentro del año siguiente a la vigencia de la misma, es decir, 29 de diciembre de 2002 se pongan al día en obligaciones por cuya causa hubiesen sido reportadas a los bancos de datos tendrán un alivio consistente en la caducidad inmediata de la información negativa histórica, sin importar el monto de la obligación e independientemente de si el pago se produce judicial o extrajudicialmente.

Esta regla general fue precisada por decreto reglamentario que estableció que para acceder al mencionado alivio el deudor debería pagar *íntegramente* las obligaciones por las cuales hubiese sido reportada. El alivio fue explicado en el sentido de que toda la información negativa histórica no tendría ningún efecto, por lo cual no podría utilizarse para negar un crédito. Los bancos de datos en todo caso podrán conservar en sus archivos la información[70].

Estos casos reflejan la importancia del debate entre el derecho de la intimidad y la información. El incumplimiento de las reglas legales y de la interpretación constitucional respecto del habeas data puede acarrear la responsabilidad personal y patrimonial tanto de las entidades financieras como de sus administradores. Para la jurisprudencia colombiana puede ser motivo de orgullo la batalla de interpretación judicial que llevo a construir la doctrina de la caducidad del dato, ahora recogida por el legislador. Hacia el futuro será interesante que este debate alcance el sector de la salud y la relación entre los datos personales y los riesgos asegurados.

g. posibilidades y límites de interceptación del correo electrónico en colombia

El avance tecnológico puede tener una faceta negativa por la utilización, por ejemplo, de medios electrónicos para la comisión de hechos punibles. En el caso del correo electrónico se contraponen por una parte la protección de la intimidad de los individuos y por otra la seguridad pública ya que en ciertos eventos las autoridades judiciales y la Fiscalía deben gozar de las prerrogativas para reprimir las actividades ilícitas cometidas utilizando las redes de telecomunicaciones e internet.

El artículo 15 de la Constitución establece que la correspondencia y demás for-

68. Corte Suprema de Justicia, Sala de Casación Penal, Sentencia 10580 del 22 de enero de 2002, M. P.: Fernando Arboleda R.

69. Ley 716 del 24 de diciembre de 2001, en *Diario Oficial*, n.º 44.661, 29 de diciembre de 2001.

70. Decreto 181 del 31 de enero de 2002.

mas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley. Por su parte la Ley 527 de 1999 establece que el correo electrónico es un ejemplo de mensaje de datos. Otros ejemplos de mensajes de datos la mencionada ley señala expresamente al intercambio Electrónico de Datos (EDI), Internet, el telegrama, el télex o el telefax. A los mensajes de datos se les atribuye el mismo valor jurídico y probatorio que a los documentos tradicionales según el principio de equivalencia funcional del artículo 6.º de la ley citada.

Con esos supuestos es interesante indagar cuales son las alternativas de investigación de un fiscal o un juez penal frente al correo electrónico. El artículo 297 del CPP establece la posibilidad de retener correspondencia privada, postal o telegráfica que el implicado en un hecho punible reciba o remita. En ese caso, una aplicación adecuada al espíritu de la norma sugiere que también sea posible incluir al correo electrónico sobretodo porque todas esta forma de comunicación han sido incluidas en la noción de mensaje de datos de la Ley 527 de 1999. Lo mismo pasaría respecto al artículo 298 relativo a la solicitud de copias de comunicaciones telegráficas. Es decepcionante que un código de procedimiento penal del siglo XXI –dos años posterior a la ley de comercio electrónico– haya desconocido la realidad dando relevancia al telégrafo, creando cierta incertidumbre jurídica, cuando la realidad indica que cada día es el correo electrónico el medio más económico y eficiente para la comunicación privada.

Pareciera ser que la *interceptación de comunicaciones prevista en el artículo 301 del CPP* sería la facultad más eficiente para el funcionario judicial respecto del correo electrónico. Los límites establecidos por la norma son los siguientes (1) el único objeto es el de buscar pruebas judiciales, (2) se pueden interceptar mediante grabación magnetofónica las comunicaciones telefónicas, radiotelefónicas y similares que utilicen el espectro electromagnético, que se hagan o reciban y (3) 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. Tales grabaciones se trasladaran al expediente, por medio de escrito certificado por el respectivo funcionario.

Es necesario puntualizar que la norma se refiere a comunicaciones similares a las telefónicas y radiotelefónicas por lo cual a primera vista se podría afirmar que es posible interceptar el envío y recepción de correo electrónico. Sin embargo la grabación magnetofónica no sería la herramienta apta para la interceptación del correo electrónico como tampoco es evidente que un servicio de correo electrónico siendo de valor agregado utilice directamente espectro electromagnético. En todo caso, y si llegar a aplicarse esa norma los proveedores de servicios de internet deberían realizar la misma en el término perentorio establecido por el legislador.

Otro problema importante a tener en cuenta es que muchos de los servidores y plataformas tecnológicas de los proveedores de servicios de correo están ubicadas en el extranjero. Lo anterior puede dificultar la aplicación de las medidas solicitadas por el Fiscal o Juez al proveedor de servicios nacional o a la sucursal del PSI extranjero. La sana lógica indicaría que sea el origen del mensaje de datos el que de-

termine la conexión del mensaje a un territorio determinado y por ende la aplicación necesaria de las ordenes judiciales respectivas en el país de origen. Ante tanta paradoja no se debe olvidar que el U.S. Patriot Act expedido luego del 11 de septiembre si permite la aplicación extraterritorial de la ley americana, por ejemplo, para la interceptación de correo electrónico de ciudadanos colombianos –incluso si su cuenta de correo electrónico ha sido "abiertas" en Colombia– implicados con actos que afecten la seguridad nacional de ese país y esos mensajes de datos pueden ser pruebas eficaces ante los tribunales norteamericanos.

Finalmente , y para tranquilidad de los abogados defensores el articulo 299 del CPP establece que la apertura de la correspondencia interceptada –del e-mail– se dispondrá por medio de providencia motivada y se practicará con la presencia del imputado o de su defensor.

H. LAS TÉCNICAS DE BIOMETRÍA

La biometría es una forma de identificar plenamente a una persona mediante la medición de una característica física o una conducta y su posterior comparación con la de otros individuos. La identificación por la retina es la más difundida pero se puede realizar con cualquier parte del cuerpo humano. Tiene la ventaja en relación a los números de identificación digital en que no puede ser olvidada o perdida.

La biometría permite la creación de perfiles digitales que pueden ser combinados y comparados con bases de datos que contienen por ejemplo las características faciales o genéticas de los individuos, constituyéndose por ende en un instrumento de control social.

En el siglo XIX, en los albores de la neurología se ensayaron varios aparatos que conectados con el cerebro emitían vibraciones que permitían determinar si el culpable de un hecho mentía o no. Apareció luego el polígrafo, aparato que mide determinados parámetros fisiológicos de los individuos y que permite determinar con alto grado de certeza si alguien esta diciendo la verdad o mintiendo respecto de un hecho determinado, su uso se extendió no solamente al ambiente judicial sino también laboral[71].

Bien es sabido la utilización de los órganos de la visión y la huella como formas de identificación plena de un individuo en los controles de seguridad. En nuestro medio Bancafé avanza en la utilización de la biométrica como herramienta para difundir la banca electrónica en los pueblos cafeteros, donde la población de bajo nivel educativo no tendrá que aprender claves de sus cuentas, pues la identificación se realizará con la huella digital[72].

Los datos no solamente se refieren a características personales externas como el nombre o la raza, con la creciente influencia de la genética se ha desarrolla do la bioinformática que es un híbrido entre la biología y la genética permitiendo la investigación sobre el genoma humano mediante la utilización de bases de datos por ejemplo de millones de combinaciones de bases nitrogenadas que constituyen la arquitectura del genoma.

71. SEAN O'CONNOR. "Collected, tagged and archived: Legal Issues in the burgeoning Use of Biometrics for Personal Identification", *Stanford Technology Law Review*, Working papers en [http://stlr.stanford.edu/STLR/Working_Papers/98_O_Connor_1/index.htmllb].

72. *Revista Dinero*, n.º 148, 14 de diciembre de 2001, p. 33.

El cuerpo humano se convierte entonces en un conjunto de datos que debe ser protegido de los abusos de terceros. El perfil genético de un individuo, el retrato y la imagen, los hábitos y costumbres hacen parte de la vida privada deben ser objeto de protección adecuada por el derecho público y privado

El caso del retrato es definido en la ley de derechos de autor[73]. Toda persona tiene derecho a impedir que su busto o retrato se exhiba o ponga en el comercio sin su consentimiento expreso, o habiendo fallecido ella, de los herederos. La persona que haya dado su consentimiento podrá revocarlo con la correspondiente indemnización de perjuicios

Esta hipótesis hace referencia a la faceta patrimonial de la imagen de los individuos. Lo anterior explica que el legislador haga referencia expresa a la posibilidad de un daño a terceros en el evento que estos por ejemplo hayan realizado inversiones económicas como consecuencia de la autorización.

La regla general de la propiedad del retrato de uno mismo tiene excepciones En efecto, la publicación del retrato es libre cuando se relaciona con fines científicos, didácticos o culturales en general o con hechos o acontecimientos de interés público o que se hubieren desarrollado en público.

Se debería entender que la noción de interés o desarrollo en público se debería interpretar de manera restrictiva por cuanto su razón de ser es proteger la libertad de información y no, intereses particulares. El uso del retrato para fines de seguridad y demás aplicaciones de la biometría hace necesario una regulación independiente de la actualmente prevista en la legislación del derecho de autor.

CONCLUSIONES

1. Los datos son parte esencial de la vida moderna. La sociedad de la información que nos prometen propios y extraños es la consecuencia de un flujo ininterrumpido de datos sobre personas y cosas.

2. Las bases de datos permiten el almacenamiento de los datos para su uso comercial, social y político. Diversas categorías jurídicas protegen las bases de datos. Como compilación, las bases de datos son protegidas por el derecho de autor. Su carácter comercial ha forzado que otras ramas del derecho protejan la información, por ejemplo, el derecho de la competencia.

3. La convergencia de diversos regímenes de protección no ha llegado a proteger los datos mismos de manera directa

4. Los derechos de los propietarios de las bases de datos se contraponen en muchos caso a los propietarios de los datos que forman parte de las primeras. Propiedad, derecho de información e intimidad son las nociones que pueden servir para resolver el conflicto

5. El derecho de la intimidad protege los derechos de rectificación y guarda de los datos personales de los individuos

6. La intimidad es amenazada por intereses comerciales y políticos que deben ser medidos caso por caso para evaluar el necesario equilibrio entre intimidad e información.

7. Las nuevas tecnologías aumentan el interés en discutir la propiedad de los datos pues los instrumentos materiales crea-

73. Artículos 36 y 88 de la Ley 23 de 1982.

dos como internet y el ciberespacio propician que un mayor control social, en particular a partir de la utilización y manipulación de los datos personales

8. Casos específicos nos demuestran que la intimidad y la información están en constante tensión. La forma de articular tales derechos puede ser definida por el legislador o por el juez, Es necesario que el artículo 15 de la constitución sea reglamentado para incluir una regulación específica de la intimidad en los casos más relvantes.

9. La biometría y la información genética son una nueva frontera para la discusión sobre la propiedad de los datos.

10. La reflexión sobre la naturaleza de la protección de los datos apenas comienza. Inicialmente las bases de datos solo protegían la selección de los datos, luego el derecho de la competencia y el secreto empresarial protegieron el valor comercial de la información. La intimidad y el derecho de la información protegen a los individuos y a sus datos personales.