Seguridad y privacidad o seguridad vs. privacidad, ¿compatibles?

En este artículo se hablará del tema de la privacidad desde la perspectiva de la legislación colombiana aplicable, los pronunciamientos jurisprudenciales que ha habido, su aplicación en la empresa y una parte de conclusiones.

Rafael Hernando Gamboa Bernate [1]

Cuando pensamos en seguridad de sistemas de información, se piensa sobre todo y casi exclusivamente, en la protección de una estructura e información, sin detenernos a pensar en cómo logramos el fin, seguridad, sin preocuparnos por los medios.

Dentro de los "medios", se encuentra la privacidad de las personas que participan en la cadena que procura la citada seguridad.

En Colombia, tradicional e históricamente, la privacidad no había tenido mayores desarrollos, contrario a otras latitudes, estuvo circunscrito a un factor de seguridad y netamente económico. Yo no quería que se supiera cuál era mi patrimonio, porque podría volverme un objetivo de bandas delincuenciales.

El que las personas supieran mis datos diferentes a los financieros, no me generaba mayor intranquilidad y es así como aún hoy, entrego muchísima de mi información a cambio de un descuento, una camiseta, una calcomanía, una cara bonita o simplemente porque me la piden. Nunca me detengo a pensar ni mucho menos a preguntar, quién la va a tener, para qué, con qué seguridad va a contar o a quién y para qué se la va a entregar.

Por mucho tiempo, toda esta información se guardaba e indexaba en unas bases de datos, de una forma muy básica y limitada, no sólo por la dificultad que implicaba su traspaso, sino porque su uso era bastante restringido, así como el de sus cruces, casi inexistentes.

[1] Las expresiones expresadas en el presente artículo corresponden exclusivamente al autor y no responden de manera alguna, ni refleja el pensamiento de las entidades con que ha tenido y tiene relación.

Con el desarrollo de los sistemas de información y de las comunicaciones, a estas bases de datos les crecieron las finalidades de uso e interesados. Al estar indexadas y en formato electrónico, se permitió su cruce, almacenaje, realización de perfiles y su envío, de una manera muy eficiente y exacta.

Dentro de la información "privada" o de datos personales, se incluye toda aquella que de una manera directa o indirecta puede identificar, individualizar o agrupar a una persona en un segmento determinado. Unos ejemplos de esta información son los datos biográficos, raza, familiares, direcciones IP, domicilio, laborales, política, hobbies, financiera, estado civil, afiliaciones, impuestos, bienes, sanciones, sexo, genética, hijos, salarios, alcoholismo, deudas, calificaciones, viajes, talla, colores favoritos, gustos, salud, tarjetas de crédito, datos biométricos, estrato, religión, cumplimiento de obligaciones entre otros… es decir, todo.

La finalidad de este escrito, no es hablar de la seguridad, de ese tema se ocuparán en este número personas más calificadas. En este artículo se hablará sobre la privacidad, desde la perspectiva de la legislación colombiana aplicable, los pronunciamientos jurisprudenciales que ha habido, su aplicación en la empresa y una parte de conclusiones.

No se busca que sea un manual, se busca por un lado sentar la alerta de que la privacidad es un aspecto bien delicado, al que hay que prestarle atención y por otro, poner de presente los principales aspectos que se deben tener en cuenta, al tratar y manejar información que potencialmente sea objeto de privacidad.

1. Regulación en Colombia

Constitución Nacional

En el artículo 15 de la Constitución que nos rige desde 1991, se establece lo que se conoce como el derecho del *Hábeas Data*, o el derecho que tienen todas las personas de conocer y controlar la información que sobre ellos reposan en los bancos de datos y archivos de entidades públicos y privados.

Dice el artículo 15 de la Constitución colombiana:
"*ARTÍCULO 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.*
En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.
La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.
Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley".

La pregunta que surge es, si este derecho existe de manera expresa en la Constitución de 1991, ¿por qué sólo hasta ahora es un tema que se menciona tanto? La respuesta, como se dijo en la parte introductoria, es porque el desarrollo de la tecnología, por el vacío normativo y la integración internacional, demanda de un tiempo para acá, un desarrollo regulatorio más amplio que el que se venía presentando.

Efectivamente, la gran mayoría de los desarrollos del citado artículo 15 de la Constitución, se daban vía tutela, cuando una persona solicitaba un crédito y la

entidad verificaba en las centrales de riesgo y al encontrar que estaba "reportada", procedía, entre otros criterios[2], a rechazar el crédito.

Ante el rechazo del crédito, por estar reportada, se iniciaron muchísimas acciones de tutela en contra de las centrales de riesgo, que, al amparo del artículo 15 de la Constitución, le ordenaba a la central de riesgo o "Cifin" y "Datacrédito", retirar a la persona.[3]

Ley de Hábeas Data I

Ante esta situación, las Centrales de Riesgo y el Gobierno nacional interesados en fijar políticas de protección de datos personales para cumplir con estándares europeos de protección y poder ser sede de callcenters, promovieron una iniciativa legal que concluyó en la ley estatutaria 1266 de 2008: "Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones".

Esta Ley Estatutaria 1266 de 2008, básicamente lo que regula es: (i) unos principios de veracidad, finalidad, circulación restringida, temporalidad, interpretación integral, seguridad y confidencialidad de la información, (ii) la forma de circulación de la información, (iii) la determinación, alcance, derechos y obligaciones de los operadores, la fuente y los usuarios.

Esta ley regula la forma y es un verdadero "manual de procedimiento" de la información de los ciudadanos. Es importante recordar que el artículo 18 establece las sanciones ante el incumplimiento así:

"*ARTÍCULO 18. SANCIONES. La Superintendencia de Industria y Comercio y la Superintendencia Financiera podrán imponer a los operadores, fuentes o usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países previas explicaciones de acuerdo con el procedimiento aplicable, las siguientes sanciones:*
Multas de carácter personal e institucional hasta por el equivalente a mil quinientos (1.500) salarios mínimos mensuales legales vigentes[4] *al momento de la imposición de la sanción, por violación a la presente ley, normas que la reglamenten, así como por la inobservancia de las órdenes e instrucciones impartidas por dicha Superintendencia. Las multas aquí previstas podrán ser sucesivas mientras subsista el incumplimiento que las originó".*

"*El año pasado, la Superintendencia de Industria y Comercio (SIC), impuso multas relacionadas con mal manejo de información por 2.300 millones de pesos y, en los cuatro primeros meses de 2012, las sanciones ya van en 825 millones de pesos*".[5]

Aunque esta ley pretendió cobijar la protección íntegra del hábeas data que trata el publicitado artículo de la Constitución, en la revisión constitucional, así como en sendos conceptos de la Superintendencia de Industria y Comercio y de la Superintendencia Financiera, se afirmó que la ley 1266 de 2008 sólo aplica para información concerniente al surgi-

[2] La Superintendencia Financiara, antes Bancaria, ha proferido varias circulares donde instruye a las entidades de crédito que no puede rechazar una solicitud, "por el solo hecho" d estar reportada la persona, sino que debe hacer una análisis íntegro del solicitante.
[3] Es importante que estas centrales de riesgo, lo único que hacen es recibir la información que le proporcionan empresas.
[4] Equivalen al 2012 a $951´750.000 aproximadamente.
[5] www.portafolio.co Mayo 27 de 2012 http://www.portafolio.co/economia/colombia-aprieta-clavijas-proteccion-hábeas-data

miento, cumplimiento y extinción de obligaciones dinerarias.

Ley de delitos informáticos

Se afirma que "el derecho sigue a los hechos", quiere decir lo anterior que las normas lo que hacen es regular situaciones que se den en la sociedad.

Los hechos actuales son tecnológicos, por lo que la regulación tendrá que entrar a regular los hechos tecnológicos. En el sector financiero, históricamente el más atacado por piratas informáticos, se vio en la necesidad de regular las actividades que causaban un perjuicio mediante el empleo de herramientas informáticas.

La preocupación del sector financiero se incrementó al ver que las actividades ilícitas en contra del sistema financiero, estaban siendo desechadas por el órgano judicial, al considerar que no existía regulación aplicable a los "delitos informáticos".

Por lo anterior, se presentó y expidió la ley 1273 de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

La finalidad de esta regulación fue establecer como delito las actividades que se cometieran utilizando herramientas electrónicas. Las normas que hay son:

"*Artículo 269A: Acceso abusivo a un sistema informático.*
Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.
Artículo 269C: Interceptación de datos informáticos.
Artículo 269D: Daño Informático.
Artículo 269E: Uso de software malicioso.
Artículo 269F: Violación de datos personales.
Artículo 269G: Suplantación de sitios web para capturar datos personales.
Artículo 269H: Circunstancias de agravación punitiva:
Artículo 269I: Hurto por medios informáticos y semejantes.
Artículo 269J: Transferencia no consentida de activos."

En esta clasificación y con relación directa a la seguridad, llaman la atención los artículos 269A y 269F. En el primero, se establecen dos criterios, el abuso y el romper medida de seguridad; es decir, si existe un oficial de seguridad podrá hacerlo sin que se incurra en lo establecido, toda vez que cuenta con autorización (desvirtuando el abuso); y, acceder sin necesidad de romper seguridad, por tener un perfil de superusuario.

En cuanto al artículo 269F, se establece que:

"Artículo 269F: *Violación de datos personales*. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes".[6]

Como se ve, los delitos tipificados nada tienen de novedoso, son simplemente la materialización de hechos y actividades ya existentes, como son el hacking, DoS,

[6] Equivalente de $63´450.000 a $634´500.000 en el 2012.

virus, troyanos, phishing, realización, manipulación y uso de datos personales entre otros.

Ley de Hábeas Data II

Frente a la limitante de ser la Ley 1266 de 2008 sólo para obligaciones financieras y al persistir la necesidad e interés de regular toda la demás información no financiera, está en trámite el proyecto de ley estatutaria No.184 de 2010 Senado, 046 de 2010 Cámara, por el cual se dictan disposiciones generales para la protección de datos personales.[7]

Este proyecto está en la Corte Constitucional y ya tuvo visto bueno, se espera que en los próximos meses sea enviado a la Presidencia para su respectiva sanción.

Este proyecto una vez sea proferido, entrará a regular todos los aspectos relacionados con cualquier tipo de información y bases de datos, excluida la financiera y trae igualmente sanciones así: "a) Multas de carácter personal e institucional a favor de la Superintendencia de Industria y Comercio hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes[8] al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó".

Como se ve, todas aquellas personas que posean datos o bases de datos de terceros y que no cumplan con lo que dispone la ley, se podrán ver inmersas en las responsabilidades y sanciones antes mencionadas.

2. Pronunciamientos jurisprudenciales en Colombia

Con relación a la privacidad, vía de tutela, la Corte Constitucional ha proferido un par de sentencias donde, en resumen, se ha protegido que, aun habiendo acuerdos y suscripción de políticas, la intimidad de las personas, respecto de los equipos de cómputo es inviolable.

Fue así como se protegió "…*la intimidad, la honra y al buen nombre, así como a la autodeterminación sobre su propia imagen*…" por fotos de contenido sexual, encontrados en equipo de cómputo de la empresa, a pesar de haberse suscrito una política que establecía la expresa prohibición de usar los equipos par asuntos privados.[9]

En otro caso ante una orden de un juez de sacar copia de los correos institucionales, no se vulneró "… *la intimidad o a la inviolabilidad de la correspondencia" cuando se obtienen copias electrónicas dentro de un proceso y bajo el mandato del juez*".[10]

Dentro de un proceso, se aportaron unos correos electrónicos enviados por el demandado y la Corte Constitucional, protegió "…*la intimidad, debido proceso y acceso efectivo a la administración de justicia…" por correos electrónicos obtenidos sin autorización judicial.*[11]

Como se desprende de lo anterior, en Colombia, existe un criterio constitucional unificado en la línea que por cuenta del artículo del Hábeas Data de la Constitución, no existe causal ni justificación alguna para que so pretexto de la seguridad, se vulnere la privacidad de las personas.

3. Desarrollos internacionales

A nivel internacional y en aras del tiempo y del espacio de este artículo, basta con afirmar que en la actualidad y como

[7] http://www.hábeasdata.org.co/wp-content/uploads/2010/12/Informe-Conciliaci%C3%B3n1.pdf
[8] Aproximadamente $634´500.000, para el 2012.
[9] C.C. 24-May.-07 M.P. Jaime Córdoba Triviño.
[10] HCSJ 4-Sep.-07 M.P. Arturo Solarte Rodríguez.
[11] C.C. 18-Sep.-08 M.P. Clara Inés Vargas Hernández.

consecuencia de muchas condenas en contra de las empresas y organizaciones, los empleados no deben esperar ningún tipo de privacidad, cuando empleen herramientas, correo o conexiones de la empresa u organización.

La anterior conclusión, extraña para nuestra cultura jurídica, fue el resultado de analizar la responsabilidad de una empresa por algún actuar de su empleado, frente a lo que se concluyó que no había sido lo suficientemente diligente, en el control y monitoreo de la actividades de sus empleados.

4. Aplicación en la empresa

Al estar dentro de una organización, se debe evaluar cómo realizar mejor nuestro trabajo, sin que se vulneren los derechos de los trabajadores.

Uno de estos derechos que cobra cada vez más relevancia es el de la privacidad, la cual puede verse seriamente afectada por políticas de seguridad que deba implementar la organización.

Dicho de otra manera ¿cómo puedo hacer bien mi trabajo de seguridad, si precisamente un aspecto muy importante es tener la capacidad de monitorear actividades que sean potencialmente riesgosas a los sistemas de una organización? La respuesta sale de la pregunta misma ¿cuál es el fin? La seguridad; ¿cuál es el medio? Supervisar; ¿puedo verme enfrentado a potenciales demandas legales por la supervisión? La respuesta es sí. Finalmente, ¿qué probabilidades tengo de perder las demandas? Altas, y ¿entonces?

Hay que hacer un análisis sobre los eventuales riesgos frente a la potencialidad de reclamaciones judiciales, las cuales serán en su mayoría acciones de tutela.

Una última pregunta ¿cuál es la finalidad y obligación del gerente de seguridad?

***Rafael Hernando Gamboa Bernate**. Abogado de la Pontificia Universidad Javeriana de Bogotá. Master en leyes (LL.M.) en Tecnologías de la Información y Privacidad de The John Marshall Law School Chicago. Master en leyes (LL.M.) en Propiedad Intelectual de The John Marshall Law School Chicago. Ha sido Profesor de posgrado en la Universidad de los Andes, UPB Bucaramanga, UPB Medellín, Universidad de Antioquia, Universidad Javeriana Bogotá, Universidad Externado, Universidad del Rosario, Universidad de la Sabana, Universidad Sergio Arboleda. Trabajó con el Centro de Arbitraje y Conciliación de la Cámara de Comercio de Bogotá, también trabajó con el Consorcio Canales Nacionales Privados de Televisión Caracol Televisión y RCN Televisión. En la ciudad de Chicago trabajó con el Latinamerican Legal Initiatives Council -LALIC- del American Bar Association. Arbitro de la Cámara de Comercio de Bogotá, Miembro del Instituto Colombiano de Derecho Procesal. Miembro del Grupo GECTI de la Universidad de los Andes. Es asesor del Banco Mundial y del Banco Interamericano de Desarrollo en temas de justicia. Actualmente es miembro de la oficina de Abogados Bernate & Gamboa Abogados. rhgb@bernateygamboa.com y Socio Fundador de la empresa de consultoría.*