A Timely Analysis of Legal Developments

ASAP®

29 de julio de 2013

Colombia Adopta Normas Sobre la Protección de Datos Personales

Geida Sanlate, Philip Gordon, Santiago Martinez Méndez, Juan Carlos Varela

Con la promulgación de nuevas regulaciones sobre la protección de datos personales, las empresas que operan en Colombia deben acogerse a estas políticas e implementarlas en sus empresas, para acatar la ley de privacidad colombiana. En octubre del 2012, se promulgó en Colombia la ley 1581,[1] la cual se encarga de regular la protección de datos personales, y de esta manera, salvaguardar el derecho constitucional a la privacidad en una época de cambios debido a la globalización y las nuevas tecnologías que de una manera más sencilla permiten la transferencia de esta información a través de medios electrónicos. El 27 de junio de 2013 a través del Decreto 1377[2] (el cual entró en vigencia a partir de su promulgación) el Gobierno reglamentó la Ley 1581. Este artículo plantea los aspectos a tener en cuenta fruto de las nuevas obligaciones de la Ley 1581 y el Decreto 1377, así como las posibles sanciones que podrían ocurrir de no acatar estas nuevas normas. De igual manera, este artículo proporciona recomendaciones para que las empresas puedan cumplir completamente con la ley de privacidad.

La Ley 1581 forma parte de una nueva tendencia, la cual está cogiendo fuerza en Latino América, que establece nuevos regímenes en la protección de datos personales. Para el momento de esta publicación Colombia se une a Argentina, Costa Rica, México, Perú y Uruguay, en la promulgación de leyes de esta naturaleza. Otros países como Brasil, están contemplando este tipo de leyes. Las empresas multinacionales que tengan empleados en América Latina deben comenzar a alinearse con estas nuevas tendencias.

El derecho constitucional a la privacidad

A partir de la constitución Política de Colombia de 1991, todos los ciudadanos tienen derecho inviolable y fundamental a la privacidad tanto personal como familiar, y a la protección de su buen nombre. Hasta que fue expedida la Ley 1581, la Corte Constitucional Colombiana interpretó e hizo exigible este derecho a la privacidad, dejando abierto el entendimiento de este derecho fundamental a la interpretación de las compañías a partir de los antecedentes jurisprudenciales.

En intento de crear un marco jurídico uniforme para la protección de los datos personales, la Ley 1581 recoge y codifica los pronunciamientos judiciales de las decisiones sobre el tema e impone requisitos para garantizar que las entidades públicas y privadas, al recolectar, procesar y/o

1 Ley 1581, "Disposiciones Generales para la protección de datos personales" promulgada el 17 de octubre de 2012.

2 La Superintendencia de Industria y Comercio emitió el Decreto 1377 el 27 de junio de 2013.

transferir datos personales, lo hagan sin atentar contra dicho derecho constitucional. La Ley 1581 a su vez deja claro acerca del derecho de acceder, corregir y revisar el uso de la información personal que se les garantiza a todos los habitantes, sin importar la edad o el sexo, y en todos los ámbitos de la sociedad, incluyendo el lugar de trabajo.

Previsiones importantes de la ley de datos personales

La ley de protección de datos personales impone varias obligaciones de la parte responsable que directa o indirectamente haga tratamiento de datos personales respecto del titular de ésta. La Ley 1581 define a la parte responsable como al individuo o entidad público o privado que haga tratamiento de datos personales, o decida como procesar los datos o cómo asegurar la base de datos. El titular de la información es el individuo, al que su información personal ha sido objeto de tratamiento. El tratamiento de los datos personales incluye la recolección, procesamiento, almacenamiento, uso, transferencia o la supresión de cualquier información que pueda estar asociada con un individuo identificado o identificable.

Debido a que como parte de su curso normal del negocio, por lo general los empleadores recogen y tratan los datos personales de sus trabajadores potenciales, actuales o ex trabajadores, los empleadores deben ser conscientes de las siguientes disposiciones:

Aviso de Privacidad. Independientemente de que sea de manera escrita, verbal o electrónica, la parte responsable debe notificar al titular sobre: (i) El propósito del procesamiento de los datos; (ii) El propósito del uso de la información personal; (iii) Los derechos de privacidad del titular; y (iv) la manera como el titular puede acceder a las políticas de la parte responsable, sobre el procesamiento de la información personal. Para efectos de comprobar que los trabajadores entendieron el aviso, consideramos que debe estar en español, explicado en una manera clara y sencilla.

Requerimiento del consentimiento (en general). La parte responsable debe obtener la información del titular, con consentimiento previo e inequívoco sobre el tratamiento de sus datos personales. Para que el consentimiento sea válido, debe ir acompañado de un aviso de privacidad en la que se detalle lo señalado con anterioridad. El consentimiento debe ser expreso, y se puede proporcionar por escrito, verbalmente o por medios que quede clara la autorización del titular al tratamiento de su información personal. Sin embargo, en ningún caso el silencio puede ser entendido como consentimiento expreso. Se le recomienda a los empleadores que en lo posible busquen obtener una firma de consentimiento, para así poder establecer el consentimiento expreso del titular.

La ley establece que la parte responsable debe mantener prueba del consentimiento inequívoco. La ley de privacidad no es del todo clara en cuanto al tiempo que la parte responsable debe preservar la prueba de consentimiento. De cualquier modo, sería prudente que los empleadores implementen procedimientos para mantener archivada las pruebas y registros de la autorización del tratamiento de la información por los últimos tres años, a partir de la fecha en que la relación laboral finalice, pues coincide con el término de prescripción para la reclamación de otros derechos laborales.

El consentimiento puede ser revocado en cualquier momento, excepto que la información suministrada sea para el cumplimiento de un deber legal o reglamentario. La parte responsable debe proporcionar un procedimiento para que el titular pueda revocar de manera fácil y sin costo la autorización. Sin embargo, si en cualquier momento el tratamiento que se le de a los datos personales excede la finalidad para la cual fueron obtenidos, el titular de estos tendrá el derecho de solicitar a la SIC, a la agencia de regulación encargada de hacer efectiva esta ley, ordenar la revocatoria y supresión de la información.

Consentimiento para el tratamiento y la protección de los datos personales sensibles. Excepto en determinadas circunstancias, procesar datos personales sensibles es prohibido. Datos sensibles se refiere a todo tipo de información íntima sobre el titular, como características que se refieran a su origen racial o étnico, condiciones médicas, los datos relativos a la vida sexual, filiación política, religión o creencias filosóficas, si pertenece a un sindicato o a una organización de derechos humanos o información biométrica. Debido a que los datos sensibles pueden ser utilizados indebidamente para discriminar en contra de las personas, la ley de privacidad establece que ninguna actividad podrá condicionarse a que el titular suministre datos personales sensibles. Esto significa que a un empleador no se le permite requerir que un actual o futuro trabajador proporcione su información personal sensible para la

contratación o continuar el contrato de trabajo, a no ser que el empleador deba cumplir con un mandamiento legal en la recolección de esta información, como es el caso, por ejemplo, cuando se requiere conocer la condición de salud del trabajador para poder desarrollar una determinada actividad.

Asumiendo que es permitido recolectar y procesar información personal sensible, la parte responsable en todo caso deberá asegurar que la información es protegida adecuadamente y mantenida de forma confidencial.

El tratamiento o uso de la información personal es limitado. Inclusive con el consentimiento del titular de la información, la parte responsable sólo puede procesar la información por un tiempo limitado, exclusivamente para los fines que el titular ha autorizado. Una vez la necesidad de la autorización se satisface, la parte responsable deberá suprimir los datos personales, a no ser que requiera mantenerse para cumplir con un deber legal, contractual o administrativo. Bajo este entendimiento, pueden existir justificaciones legítimas para que los empleadores puedan preservar y acceder a información personal de sus trabajadores actuales y ex trabajadores durante el tiempo que requiera dar cumplimiento a obligaciones sobre la desvinculación y seguridad social del trabajador.

Transferencia internacional y de otros tipos, de datos personales. Siempre que la parte responsable transfiere datos personales a un tercero, tal como personas que administran bases de datos para diversos fines (como puede ser para fines comerciales), la parte responsable debe celebrar un acuerdo con el tercero para que éste sólo utilice la información con los fines para lo cual el titular de la información autorizó. Esto implica que la información no puede ser tratada para fines diferentes a los que expresamente autorizó.

La ley bajo estudio es clara en materia de transferencia internacional de los datos personales, como cuando una subsidiaria ubicada en Colombia transfiere datos personales a casa matriz ubicada en EEUU. En tal caso, la transferencia está prohibida, a no ser que el país al cual fueron transferidos los datos personales proporcione niveles adecuados de protección de datos mayores o iguales a los proporcionados por la Ley 1581. Se entiende que ofrece niveles adecuados, cuando así lo haya determinado la SIC o cuando la transferencia sea en conformidad del marco de tratados internacionales en los cuales Colombia sea parte. A la fecha de la publicación de este artículo, se desconocen lineamientos por parte de la SIC respecto de si Colombia considerará que las normas del convenio "Safe Harbor Framework" entre EEUU y la Unión Europea para la protección de datos, proporcionan niveles adecuados de protección de datos.

Sin embargo, existen una serie de excepciones. Dos de ellas que cabe mencionar son cuando: (a) el titular de la información autoriza expresamente la transferencia internacional de los datos y; (b) cuando la transferencia se requiere para el cumplimiento de una obligación legal o contractual.

Disponibilidad de políticas internas para el titular de la información. La parte responsable debe establecer e implementar políticas y métodos para la adecuada protección de la privacidad y confidencialidad de los datos personales. Se recomienda que los empleadores adopten políticas y suministren lineamientos a las áreas de recursos humanos y tecnología sobre la correcta administración de los datos personales.

Aplicación y sanciones en caso de incumplimiento. El Decreto 1377 establece que la SIC se encuentra facultada para hacer efectivo el cumplimiento de la Ley 1581 mediante la imposición de sanciones en caso de incumplimiento. La SIC podrá imponer multas por la suma de 2.000 salarios mínimos legales mensuales vigentes. Para el momento de esta publicación, la máxima multa sería por la suma de US $627,411. Otras sanciones que pueden ser impuestas es la suspensión de operaciones por hasta seis meses, cierre temporal pero indefinido de operaciones, en el evento en el que la empresa mantenga su incumplimiento, e inclusive cierre permanente de operaciones si la compañía se rehúsa a cumplir con las obligaciones legales establecidas en las normas estudiadas.

Recomendaciones

A partir de la promulgación de estas nuevas normas, Colombia ingresa en la comunidad internacional de países que han reglamentado la adecuada protección de datos personales. Con una nueva normatividad, los titulares ahora pueden gozar de mayores protecciones de su información personal y los individuos y entidades ahora requieren cumplir con nuevas y extensas obligaciones en relación con la recolección, uso y procesamiento de la información personal. Consideramos que éste es tan solo el comienzo de las reglamentaciones, pues el gobierno nacional ha anunciado su compromiso de proteger el derecho a la privacidad en medio del desarrollo creciente de la era de la tecnología.

Teniendo en cuenta que la ley aplica en todo el territorio nacional, todos los particulares o entidades que realicen tratamiento de bases de datos, se encuentran dentro del marco de las obligaciones mencionadas (salvo las excepciones que la ley establece en casos determinados). Por ello, los empleadores deben cumplir con las normas al momento de hacer tratamiento de información personal de sus trabajadores, así como al momento de hacer transferencia internacional de la misma. Por ejemplo cuando casa matriz obtiene información en Colombia para procesarla en otro país, debe asegurar que el titular de la información ha suministrado su consentimiento expreso para tal efecto.

Se espera que la SIC adelantará inspecciones para asegurar su cumplimiento, con enfoque especial en las industrias de salud y entidades financieras en consideración a lo sensible que es la información que estas entidades recolectan. Empleadores de empresas domésticas y multinacionales deberán adoptar medidas necesarias para efectos de dar cumplimiento a esta normatividad. Como parte de las medidas por adoptar, recomendamos a las compañías adoptar las siguientes:

1. Crear e implementar políticas internas para regular el correcto tratamiento y adecuada protección de los datos personales, bien sea para recolectar, procesar, almacenar, usar, transferir o la supresión de la información. Esas medidas deben tener por objetivo asegurar que la información personal sensible no será nunca pública.
2. Comunicar dichas políticas de una manera uniforme a todos los trabajadores que han autorizado el tratamiento de información personal y, obtener el acuse de recibo de parte de ellos.
3. Identificar el propósito específico para el cual la información personal será procesada.
4. Proporcionar un aviso de privacidad a los candidatos, al igual que a los trabajadores activos, que contenga la información detallada con anterioridad.
5. Obtener el consentimiento expreso e inequívoco del titular para procesar la información personal. Mantener prueba de (i) el consentimiento del titular de la información y; (ii) el acuse de recibo.
6. Haga tratamiento de la información sólo para el propósito para el cual fue recolectada y autorizada.
7. Antes de la transferencia de cualquier dato a un tercero (prestador de servicios), asegurarse que el prestador del servicio ha aceptado, contractualmente, la protección de los datos, de conformidad con las políticas de su compañía y que sólo será utilizada para los fines autorizados.
8. En consideración a que el tratamiento de los datos personales es limitado al fin para el cual fue autorizado, los empleadores que tengan datos personales de sus trabajadores, deberán abstenerse de utilizarlos en fines diferentes a los establecidos en la autorización.
9. Obtenga un acuerdo escrito con sus trabajadores que administran bases de datos con datos personales, en los que se garantice la confidencialidad de la información que conocerán. Este acuerdo podrá ser incluido como una cláusula dentro de los contratos, en los cuales se acuerde que en caso de incumplimiento será una falta grave a sus obligaciones, lo cual da lugar a la terminación del contrato de trabajo con justa causa.

Por último, como varios de los anteriores pasos lo enfatizan, es indispensable que los empleadores documenten de manera meticulosa los diferentes procesos. Tomando estas medidas, ante una eventual visita de inspección de la SIC, se tendrá la seguridad de poder evidenciar su cumplimiento. Los empleadores deben buscar acompañamiento legal de parte de expertos en ésta área, con experiencia debida para ayudar a las compañías locales y multinacionales, en el cumplimiento de esta nueva norma.

Philip L. Gordon es un socio de Littler Mendelson en la oficina de Denver, Colorado, y Director del área de práctica de Privacidad y Protección de Datos. Juan Carlos Varela es el socio director de la oficina de Littler Mendelson en Caracas, Venezuela y Co-Presidente del área de práctica para América Latina. Geida D. Sanlate es una abogado del Departamento de Manejo de Conocimientos ("Knowledge Management Department") de Littler, con enfoque especial en las leyes laborales internacionales. Agradecimiento especial a Santiago Martinez Méndez, abogado principal y líder del área de práctica de Auditoria y Due Diligence en la firma Godoy, Córdoba Abogados, S.A.S., en Bogotá, Colombia. Si usted requiere información adicional, por favor contacte al abogado Philip Gordon a pgordon@littler.com o 303.362.2858; Juan Carlos Varela a jcvarela@littler.com o 305.400.7590; Geida Sanlate a gsanlate@litter.com o 973.848.4744; o Santiago Martinez Méndez a smartinez@godoycordoba.com o 57.571.317.4628. Para información sobre Littler, favor visitar el sitio web www.littler.com.