ANÁLISIS DE LAS SANCIONES IMPUESTAS A LOS COLEGIOS POR INADECUADOS PROCEDIMIENTOS EN EL TRATAMIENTO DE DATOS PERSONALES

José Guillermo Martínez Rojas[1]

Desde el año 2016 hasta el 2023, la Superintendencia de Industria y Comercio, se han identificado unos once (11) colegios que han sido objeto de sanciones por el inadecuado tratamiento de datos personales. La gran mayoría de las indagaciones que se han presentado, han tenido como origen, una queja que interpone un particular, ante dicha entidad.

Tomando como referencia las sanciones a los colegios impuestas por la Superintendencia de Industria y Comercio -SIC-, en relación con el inadecuado tratamiento de datos personales en los colegios, se pueden señalar aquí algunos aspectos que es importante tener en cuenta, de cara a los procesos de ajuste y de implementación de todos los procedimientos que se deben seguir, de manera especial en las instituciones educativas, justamente por la naturaleza de su función, pero adicionalmente, porque en su actividad se involucra a menores de edad, lo que impone unas condiciones especialísimas para cumplir con lo dispuesto en las normas sobre el particular.

1) Principales fallas o errores cometidos por los colegios investigados y sancionados en relación con el tratamiento de datos.

En las instituciones educativas se suelen recolectar datos personales para muchas finalidades y funciones. En las instituciones educativas sancionadas, entre otros aspectos, se les han impuesto dichas sanciones porque al momento de recabar la información personal, no se solicitó la autorización de los titulares, para el tratamiento de los datos personales de los menores (los padres de familia que tienen la patria potestad), o de los trabajadores o de los contratistas mismos, ni de los datos de los propios padres de familia, con quienes la entidad suscribía contratos o realizaba actividades relacionadas con su oferta educativa. Los principales casos o situaciones tienen que ver con esta conducta son documentos como los siguientes, en los cuales no se solicitó dicha autorización:

- Formulario de admisiones.
- Formato de análisis de documentos departamento de psicología.
- Formato de admisiones-psicología.
- Formato de entrevista a padres.
- Registro de matrícula.
- Formato de permiso cambio de ruta.
- Formato de contrato de transporte padres-colegio.

---

[1] Educador y Abogado, experto en legislación para instituciones educativas. Consultor, asesor y capacitador para colegios y asociaciones de colegios del país. Puede ser contactado en los siguientes correos electrónicos: jgm.abogadoeducativo@outlook.com o en gerencia@mbeducacion.com.co.

• Contrato de transporte.
• Formato de constancia de recibo de reglamentos a empleados.
• Contrato de trabajo empleado.
• Formulario digital de contacto http://xxx.edu.co/index.php/admisiones-xxxxxxxxx/#contacto.
• Contrato de prestación del servicio educativo.
• Formato de actualización de datos.

Así mismo, las principales conductas lesivas del derecho de hábeas data son las siguientes:
• No publicar la Política de Tratamiento de Datos de la Institución o el Aviso de Privacidad para el acceso de los titulares.
• No solicitar de manera previa, expresa e informada la autorización para el tratamiento de datos personales, máxime si se trata de menores de edad.
• No contar con un manual interno o un procedimiento para la atención de peticiones, quejas y reclamos relacionado con el ejercicio del derecho a conocer, actualizar, rectificar y suprimir los datos personales o revocar la autorización por parte de los Titulares.
• No contar con manuales y procedimientos tendientes a garantizarla seguridad de la información almacenada en los equipos de cómputo disponibles en la institución.
• No haber implementado las cláusulas de confidencialidad de tratamiento de datos personales en los contratos suscritos con sus empleados y docentes, así como tampoco, cuenta con procedimientos encaminados a identificar y controlar los riesgos asociados al Tratamiento de los datos personales.
• Solicitar al representante legal del niño, niña o adolescente la autorización, previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto.
• No haber informado a los representantes legales de los niños que estaban facultados a entregar o no la información del menor, incumpliendo con el deber de solicitar la autorización en las condiciones que prevé la ley, y vulnerando el derecho a la protección de datos de los menores de edad.
• Haber realizado tratamiento de datos personales de empleados, proveedores y terceros interesados respecto de los cuales no contaba con autorización en los términos previstos en la Ley 1581 de 2012, tal como se evidencio en los formatos recolectados durante la visita de inspección.
• No documentar, implementar y monitorear una política de seguridad de la información que contenga medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a los datos personales evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
• En los contratos laborales suscritos y mediante los cuales se recolecta información, se evidenció que la entidad no recolecta ni guarda copia de la autorización, para el tratamiento de los datos personales de los maestros y del personal administrativo en general.
• No contar con las autorizaciones requeridas incluidas en el portal electrónico que recolecta la información de los estudiantes, durante el proceso de matrícula.
• De igual manera, cuando la SIC indaga si en los formularios *on line* o digitales, una entidad ha cumplido con la solicitud de autorización por parte de los titulares de los datos personales. Ella aplica procedimientos forenses para determinar desde cuándo –la fecha-, a partir de la cual, dicha entidad está solicitando la autorización de los titulares de los datos. Este procedimiento fue aplicado en una de las investigaciones que llevó a cabo para imponer una sanción a un colegio.

2) Principales prácticas inadecuadas en la implementación de la Ley 1581 de 2012 en una institución educativa.

Además de lo referido anteriormente, en donde el principal error o falla consiste en recabar información sin contar con la debida autorización de los titulares o de quienes tienen la potestad para hacerlo, existen otras situaciones o conductas o procedimientos de los colegios, de diferente naturaleza, que han sido objeto de sanciones y que aparecen en los actos administrativos mediante los cuales se imponen dichas sanciones. Las más relevantes y comunes son las siguientes:

• No haber realizado el registro de las bases de datos con que cuenta la entidad, debiéndolo haber hecho, puesto que la misma, está obligada, justamente por contar con las condiciones que las normas estipulan, para tal procedimiento. O habiéndolo hecho, no fue bien realizado.
• No contar con una política de tratamiento de datos que cumpla con las condiciones mínimas que las normas exigen para dicho tipo de documentos.
• Las autorizaciones o avisos de privacidad no cuentan con los parámetros mínimos que las normas imponen para tales documentos.
• No existen términos y procedimientos claros y precisos para tramitar las consultas y reclamos formulados por los titulares de los datos, en los términos señalados en la Ley.
• No haber adoptado un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de pedido por la Ley de hábeas data, y en especial, para todo lo relacionado con la atención de consultas y reclamos de los titulares de los datos.
• No haber informado adecuada y completamente la finalidad para la cual se solicita la autorización de tratamiento de datos.
• Solicitar una autorización sin el mínimo de aquello que dichas autorizaciones deben incluir o utilizar una "autorización sombrilla" con la cual se cubre todo el tratamiento de datos de los titulares.
• No haber desarrollado e implementado un manual de seguridad de la información, así como un manual para la atención de consultas y reclamos, un manual para la recolección, almacenamiento, uso, circulación y supresión de la información.
• No contar con manuales y procedimientos tendientes a garantizar la seguridad de la información almacenada en los equipos de cómputo disponibles en la institución.
• No tener establecido parámetros documentados para la restricción de contenidos y acceso remoto a la plataforma del colegio por parte de los educadores.
• No contar con procedimientos encaminados a identificar y controlar los riesgos asociados al tratamiento de los datos personales que se obtenían a través de los dispositivos o tabletas electrónicas que usan los profesores.
• En el caso de uno de los colegios sancionados, se determina la ocasión para la imposición de la misma, tomando como referencia los artículos anteriores afirmando que: "…*la sociedad investigada incumplió con los deberes contemplados en los literales b), c), y k) del articulo 17 de la Ley 1581 de 2012… toda vez que: (i) no solicitó y conservó, en las condiciones previstas en la Ley, copia de la autorización previa, expresa e informada de los titulares, toda vez que al momento de la visita de inspección y la entrada en vigencia de la Ley 1581 de 2012 no se encontraban en funcionamiento los formatos de autorización allegados al expediente (ii) así como tampoco informó debidamente a los titulares sobre la finalidad de la recolección y los derechos que les asisten por virtud de la autorización otorgada y en especial el carácter facultativo de las respuestas en temas de niños, niñas y adolescentes; (iii) no tenía al 25 de septiembre de 2015 un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la Ley y en especial, para la atención de consultas y reclamos (iv) y no cumplir con el deber de poner en conocimiento de los titulares las políticas de tratamiento*".
• Afirma la resolución de sanción que "*era deber de la entidad en calidad de Responsable del tratamiento de los datos, haber cumplido lo establecido en la Ley 1581 de 2012 a partir de la entrada en vigencia de la misma, es decir, a partir del 17 de octubre de 2012, y que dentro del plazo otorgado por la misma, de seis (6) meses siguientes a la entrada en vigencia de la ley, debía adecuarse para cumplir con las disposiciones contempladas en la Ley, y dentro de las pruebas aportadas es claro que dichos formatos se implementaron a partir de enero del 2018*".

• No haber implementado cláusulas de confidencialidad para el tratamiento de datos personales, en los contratos suscritos con sus empleados y educadores, así como tampoco, con aquellas personas que en virtud de alguna de las funciones o responsabilidades que deben desempeñar en el colegio, acceden a información semi-privada, privada y sensible.
• La Política de Tratamiento de Datos Personales del colegio evidencia que no contiene un procedimiento que describa los distintos momentos del ciclo de vida del dato de acuerdo con el tratamiento que se hace en la Institución Educativa, entre lo que se encuentra: (i) el método de recolección de la información; (ii) la forma de almacenamiento de la misma; (iii) los múltiples usos que puede tener la información dependiendo de las finalidades específicas para las que fue autorizada la Institución Educativa; (iv) la forma en que la información circula al interior de la Institución Educativa y si la misma es remitida a un Encargado para su Tratamiento y (v) el método empleado para dar disposición final a la información o para suprimir el dato del titular que así lo solicita.

3) Desde cuándo se debe cumplir con el tratamiento de datos.

La Ley 1581 se promulgó el 17 de octubre de 2012 y en su Artículo 28 determina que la misma entrará en vigor seis (6) meses después de su promulgación, es decir el 17 de abril de 2013. Por su parte el Decreto 1377, ahora compilado en el Decreto 1074 de 2015, que reglamentó la anterior Ley, se promulgó el 27 de junio de 2013. Sin embargo, todas las entidades que tratan datos en los términos que lo establece la Ley, ya deberían estar cumpliendo con lo prescrito en ella, desde el 17 de abril de 2013.

• Las sanciones impuestas a los colegios hacen referencia a los hechos denunciados en una queja o de oficio que la SIC adelante, para validar el cumplimiento de lo definido en las normas, por procedimientos inadecuados en el tratamiento de datos, frente a lo cual, ella se remite a lo que hay en sus bases de datos (Registro, si la Institución está obligada a hacerlo), en los documentos y procedimientos institucionales y en las evidencias que se aporten si hay una queja, o en los resultados de la auditoría que la Entidad (SIC) lleve a cabo, tales como correos, contratos, formularios, etc., en donde se evidencie cómo efectivamente la entidad sobre la que versa la queja o la investigación, estaba adelantando los procedimientos para el cumplimiento de la norma, al igual que en la información que la SIC recoge cuando visita la entidad investigada. En caso de que la queja se refiera a una situación que esté ubicada después de la fecha de la entrada en vigor de la Ley y antes de la implementación de los ajustes que se han ido haciendo a lo largo de estos años, la SIC impone la sanción por el incumplimiento de lo exigido en dichas normas.
• Según la Ley 1581 de 2012, Artículo 17, los deberes del *responsable* del Tratamiento (*Representante Legal de la Entidad*) son los que se enumeran a continuación y que se debieron implementar desde la fecha de entrada en vigencia de la Ley.

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
b) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular.
c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
e) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.

f) Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a éste se mantenga actualizada.
g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento.
h) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley.
i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.
j) Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley.
k) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos.
l) Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.
m) Informar a solicitud del Titular sobre el uso dado a sus datos.
n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
o) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

• Según la Ley 1581 de 2012, Artículo 18, los deberes del *encargado* del Tratamiento son los que se enumeran a continuación, y que se debieron implementar desde la fecha de entrada en vigor de la Ley.

a) Garantizar al Titular, en todo tiempo. el pleno y efectivo ejercicio del derecho de hábeas data.
b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
c) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley.
d) Actualizar la información reportada por los responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo.
e) Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la presente ley.
f) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los Titulares.
g) Registrar en la base de datos la leyenda "reclamo en trámite" en la forma en que se regula en la presente ley.
h) Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.
i) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.
j) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.
k) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
l) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

Los colegios realizan transmisión de datos personales a encargados que, bajo las directrices del colegio, llevan a cabo acciones con dicha información. Este es uno de los riesgos más grandes que existe para los colegios, porque dichas plataformas, de manera general, tratan mucha información sensible de la recabada por el colegio y hasta ahora, no se puede concluir que una sola de las existentes, cumpla con todas las medidas y procedimientos que se requieren para lograr un adecuado tratamiento de datos personales en el colegio y demostrar la debida diligencia en tal responsabilidad.

Igualmente, el riesgo se incrementa cuando ya no se trata de la *transmisión* de los datos personales que el colegio trata, sino cuando realiza *transferencia* de datos personales, caso este en el cual, quien recibe

los datos, los trata por su cuenta y bajo su propia política de tratamiento de datos personales, sin involucrar directamente a la entidad que le transfiere dichos datos y lo hace por su propia cuenta y riesgo.

En los dos casos anteriores es relevante precisar, que todo ello genera riesgos importantes para el colegio justamente por las obligaciones que se han enunciado anteriormente, tanto para los responsables como para los encargados de la información personal.

4) Consideraciones que se deben tener en cuenta cuando se trata de datos de menores de edad.

El tratamiento de datos personales de los menores de edad tiene importantes y definitivas características que se deben tener en cuenta, en las instituciones educativas, razón por la cual, al analizar las sanciones y lo expuesto por la SIC sobre el particular, se pueden hacer las siguientes consideraciones, sobre prácticas inadecuadas de los colegios:

• Cuando el responsable realiza tratamiento de datos personales de menores de edad, sin contar con la autorización de los representantes legales de los mismos, incurre en una práctica contraria a las normas.
• Cuando con su conducta, el colegio no garantiza la seguridad en el tratamiento de los datos personales, ni cuenta con un *Manual Interno de Políticas y Procedimientos* para garantizar el adecuado cumplimiento de la Ley, la SIC procede a imponer la respectiva sanción, por la vulneración de los deberes contemplados en el Artículo 7 (derechos de los niños y adolescentes) y los literales mencionados anteriormente del Artículo 17 de la Ley 1581 de 2012.
• Los colegios, en virtud de su labor, pueden compartir información de los estudiantes con diferentes instituciones educativas, sociedades, entidades de carácter público y privado, lo cual permite exponer datos personales de los menores, lo que puede poner en riesgo sus derechos fundamentales. Por tal motivo, en estos casos, es de obligatorio cumplimiento, contar con la autorización expresa para el tratamiento de datos personales, en los términos señalados en la Ley.
• Los colegios suelen recoger, decidir y hacer tratamiento sobre los datos personales de los menores (estudiantes del colegio), personal administrativo y educador y en general de todos sus usuarios, independiente de cuál fuese el mecanismo de recolección utilizado, cuando no cuenta o ha implementado mecanismos para recolectar la autorización de los representantes legales de los niños, niñas y adolescentes, al igual que autorizaciones del personal administrativo y educador que labora en la institución y del cual también realiza tratamiento de datos personales, ni cuenta con la autorización de tratamiento de datos personales sensibles y de menores de edad, en los términos que establece la Ley 1581 de 2012 y el Decreto 1074 de 2015.
• Teniendo en cuenta que una institución educativa incumplió el deber de solicitar la autorización previa, expresa e informada para el tratamiento, es claro entonces que tampoco cumplió con el deber de información, es decir, al momento de recolectar los datos y solicitar la autorización, debía comunicarles a los titulares: (i) el tratamiento y la finalidad de la recolección de los datos personales; (ii) el carácter facultativo de la respuesta a las preguntas que le sean hechas cuando versen sobre datos sensibles o de niñas, niños y adolescentes; (iii) los derechos que le asisten a los padres o representantes legales de los estudiantes, del personal administrativo y educador, como titulares de la información; y (iv) la identificación, dirección y teléfono del responsable del tratamiento.
• Los colegios también incumplen los principios de finalidad y libertad consagrados en los literales b) y c) del Artículo 4 de la Ley 1581 de 2012, de los cuales se desprenden los deberes de solicitar y conservar copia de la autorización previa, expresa e informar debidamente la finalidad de la

recolección y los derechos que le asisten al titular; al igual que tener un especial tratamiento de información personal de niños, niñas y adolescentes, es decir, informar al momento de la recolección de la autorización, el carácter facultativo de las respuestas, cuando las preguntas versen sobre datos sensibles o de niños, niñas y adolescentes.

• El tratamiento de datos personales de menores está permitido, siempre y cuando se acuda a una interpretación restringida, según la cual ese uso de la información se debe sujetar a la interpretación esbozada por la Corte Constitucional cuando analizó la exequibilidad del Artículo 7 de la Ley 1581 de 2012. Aun cuando el texto original de la norma estableció en principio que quedaba "*proscrito el tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública*", la Corte, en la Sentencia C-748 de 2011 aclaró que dicha disposición "*no debe entenderse en el sentido de que existe una prohibición absoluta del tratamiento de los datos de los menores de 18 años, exceptuando los de naturaleza pública, pues ello, dada lugar a la negación de otros derechos superiores de esta población (...)*". Afirma o dispone la Corte Constitucional que "*(…) en el tratamiento de los datos personales de menores do 18 años, al margen de su naturaleza, pueden ser objeto de tratamiento siempre y cuando, el fin que se persiga con dicho tratamiento, responda al interés superior de los niños, niñas y adolescentes y se asegure sin excepción alguna, el respeto de sus derechos prevalentes*".

• También estableció que "*Todo responsable y encargado involucrado en el tratamiento de los datos personales de niños, niñas y adolescentes, deberá velar por el uso adecuado de los mismos. Para este fin deberán aplicarse los principios y obligaciones establecidos en la Ley 1581 de 2012 y su decreto reglamentario*". De manera concordante con lo expuesto, en la recolección de la autorización, tal y como lo expone el literal b) del artículo 12 de la Ley 1581 de 2012, "*el responsable del Tratamiento al momento de solicitar al Titular la autorización, deberá informarle de manera clara y expresa lo siguiente: (...) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando versen sobre datos sensibles o sobre los datos de niños, niñas y adolescentes*". A la luz de lo dispuesto para el tratamiento de los datos personales de los menores, se advierte que el Colegio objeto de la sanción, no informó a los representantes legales de los niños que estaban facultados a entregar o no la información del menor, incumpliendo con el deber de solicitar la autorización en las condiciones que prevé la Ley, y vulnerando el derecho a la protección de datos de los menores de edad.

• A la luz de lo dispuesto para el tratamiento de los datos personales de los menores, la SIC identificó que el colegio en cuestión sancionado, no cuenta con una autorización disponible en el formulario electrónico habilitado en su sitio web o en físico, así como tampoco, informa la finalidad para la cual serán utilizados los datos que son recolectados y cuáles de los datos recolectados son datos personales sensibles, así como la facultad que tienen los titulares de entregar o no la información que verse sobre datos sensibles o de menores de edad, incumpliendo con el deber de solicitar la autorización en las condiciones que prevé la Ley, vulnerando el derecho a la protección de los datos de los menores de edad.

5) CONCLUSIONES Y RECOMENDACIONES PRÁCTICAS DEL ANÁLISIS DE LAS RESOLUCIONES DE SANCIÓN

A partir de lo presentado de las resoluciones producidas por la SIC para sancionar colegios que no han cumplido debidamente con lo exigido en las normas sobre la protección de datos personales, las normas sobre el particular y las sentencias de la Corte Constitucional, se pueden extraer algunas como las siguientes conclusiones y hacer también algunas consideraciones y recomendaciones para las instituciones educativas.

• El colegio que no haya implementado lo dispuesto por la Ley de hábeas data, desde el momento de entrada en vigor de la misma, 17 de abril de 2013 y sea objeto de una queja por un hecho o situación acaecida después de dicha fecha, y antes de los ajustes que haya hecho para cumplirla, así a la fecha

de hoy tenga todo al día, será objeto de la sanción, puesto que la SIC considera que debió cumplirse con lo dispuesto en la norma desde que la misma entró en vigor. Así ha sucedido con los colegios y las entidades que han sido sancionadas.

• Entre más se tarde el colegio en implementar todos y cada uno de los aspectos que impone la norma a los colegios, por tratarse de entidades cuya labor misional está dirigida a menores de edad, estarán más expuestas a una sanción, puesto que para la SIC, es un agravante el hecho de que la entidad en cuestión trate datos de menores de edad, sin las debidas medidas especiales de seguridad y demás exigencias en estos casos.

• Cuando en una entidad se traten datos sensibles, recogerlos supone que estos se requieren por razones de fuerza mayor o porque definitivamente son absolutamente necesarios para el cumplimiento de la labor misional de la entidad, en cuyo caso, se debe advertir a los titulares de dichos datos, que ellos pueden elegir libremente si los suministran o no lo hacen sin que ello le genere consecuencia alguna.

• Hay que tener un especial cuidado en las entidades que tratan datos personales de niños y adolescentes, que son menores de edad, puesto que efectivamente los datos que no sean públicos, son considerados por las normas, sensibles; pero, además, se deben extremar las medidas de protección y se debe ser absolutamente cuidadoso, sobre las razones para su transmisión o transferencia.

• La institución debe contar con *Manual Interno de Políticas y Procedimientos* para garantizar, en especial, la atención de consultas y reclamos y con ello garantizar el pleno y efectivo ejercicio del derecho de habeas data. El literal k) del artículo 17 de la Ley 1581 de 2012, contempla el deber de los responsables de adoptar, un manual interno de políticas y procedimientos cuya puesta en marcha garantice el adecuado cumplimiento de la Ley de protección de datos personales.

• Ninguna actividad de las que realiza la entidad podrá condicionarse a que el titular suministre datos personales sensibles. Ello supone una redacción adecuada en los textos de autorización a los titulares.

• La SIC recomienda a los colegios sancionados que, para evitar futuras sanciones, lo más adecuado es implementar en dichas entidades el *Principio de Responsabilidad Demostrada* contemplado en las normas, con el fin de que efectivamente se sea absolutamente diligente en la implementación de todos y cada uno de los procedimientos que garanticen todo aquello que las normas exigen.

• Los siguientes procedimientos que se llevan a cabo en un colegio, de manera habitual, son los que representan mayor riesgo para la institución, por el tipo de datos que recogen y tratan, y por la manera habitual como lo hacen; éstos son: proceso de admisiones y vinculación y desvinculación de nuevos estudiantes, proceso de selección y vinculación de empleados, procedimientos de orientación escolar, procedimientos de enfermería escolar, diligenciamiento de la información en el Registro Escolar de Valoración, diligenciamiento y tratamiento de toda la información en el observador del estudiante o en los procesos disciplinarios y convivenciales. Estos son los principales espacios en donde se pueden presentar mayores vulneraciones a los derechos de los titulares de los datos, según la naturaleza y procedimientos seguidos en una institución educativa.

• En todos los documentos, formatos, procedimientos y demás estrategias empleadas por los colegios para recabar datos personales, sean estos digitales o físicos, se deben incluir los aspectos (finalidad, el carácter facultativo de suministrar los datos si estos son sensibles o de menores de edad, los derechos que les asisten a los titulares, y, la identificación del responsable ante quien se pueden ejercer estos derechos) como mínimo.

• De igual manera, por lo conceptuado en las normas, es relevante tener en cuenta el tratamiento de los datos sensibles, entre los que se encuentran los de los menores edad, razón por la cual, si se tienen cámaras de videovigilancia, dispositivos de captura de datos biométricos como la huella, toma de fotografías, uso de las imágenes capturadas, entre otros, se debe cumplir con todo lo dispuesto sobre el particular.

• Los colegios deben hacer efectivo el pleno respeto del derecho fundamental de Habeas Data a todos aquellos de quienes ha recabado información personal, de manera especial, de los menores de edad, cuyos derechos son prevalentes, pero, además, porque ellos suelen ser los principales involucrados en el tratamiento de datos que llevan a cabo los colegios.
• En ninguna condición o situación, se pueden tratar, transmitir o transferir datos de los menores de edad, para cualquier actividad de las realizadas en un colegio, a menos que medie una autorización previa, expresa e informada, en los términos que las normas lo han dispuesto, pero, además, porque dicha actividad se lleva a cabo, en búsqueda o salvaguarda de un bien o derecho superior. Se puede llevar a cabo este tratamiento sin autorización, solamente en los términos que la Ley lo ha dispuesto o si se requiere salvaguardar un principio o derecho más importante que la salvaguarda del de hábeas dato o de la intimidad.
• Se debe hacer una revisión minuciosa de todos los formularios o formatos, sean estos en físico o digitales, en donde recoja información o datos personales de cualquier persona que entra en contacto con el colegio, pero de manera especial, aquellos en los que se involucre información de los estudiantes menores de edad, para validar que todos ellos cuenten las autorizaciones previas, expresas e informadas, o para que tengan el aviso de privacidad si es el caso, con el fin de que dicha labor de recolección de datos, esté debidamente realizada.
• No se debe olvidar que el colegio siempre estará obligado a conservar las autorizaciones que los titulares de los datos le han concedido, justamente porque dichos titulares, tienen el derecho de solicitar, de forma gratuita, en cualquier momento, evidencia de haber concedido la misma. Y para cumplir con dicha solicitud es necesario haberla conservado archivada.
• Muchos de los datos personales que se recogen y tratan en los colegios, suelen ir a documentos como libros, reportes, carpetas y archivos que la entidad debe construir o generar. No se debe olvidar que dichos documentos deben cumplir con una normatividad tripartita, a saber: las normas educativas, las normas de archivística y las normas de tratamiento de datos. Todo ello armonizado para cumplir con las exigencias de dicha tripartita normatividad.
• En la perspectiva de implementar el principio de responsabilidad demostrada, los colegios deben, entre otros aspectos, como mínimo, contar con: un programa integral de tratamiento de datos, un procedimiento de gestión del riesgo en el tratamiento de datos, un procedimiento de ciclo de vida del dato, un programa de seguridad de la información, un procedimiento para las auditorías de los procedimientos de tratamiento de datos en la institución, un procedimiento para el uso del botón PSE si la entidad cuenta con dicha opción, un procedimiento para el destino final del dato, todos ellos como mínimo.

GLOSARIO

A continuación, se propone un glosario mínimo para la adecuada comprensión del presente análisis.

Datos Privados: Es el dato que, por su naturaleza íntima o reservada, sólo es relevante para el titular. Comprende toda la información personal o familiar como por ejemplo el tipo de vínculo civil o religioso con la pareja, el nivel de escolaridad (El nivel de escolaridad, el tipo de vínculo con la pareja –civil o religioso-).

Datos Públicos: A esta categoría pertenecen los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales, debidamente ejecutoriadas que no estén sometidas a reserva (Todo lo que está en el Registro Civil o en el Documento de Identidad).

Datos Semi-Privados: Es semi-privado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación, puede interesar no sólo a su titular, sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios, para poder cumplir ciertas funciones o tareas en la sociedad (Dirección, correo electrónico, datos crediticios).

Datos Sensibles: Son aquellos datos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud como la historia clínica o psicológica, a la vida sexual y los datos biométricos (Orientación Religiosa, Política o Sexual, la pertenencia a sindicatos, o todos los datos de los menores de edad).

Principio de Responsabilidad Demostrada: Consiste en la acción según la cual, una entidad que recoge y hace tratamiento de datos personales debe ser responsable del cumplimiento efectivo de las medidas que implementen los principios de privacidad y protección de datos personales que ha recabado y trata. Igualmente, se lo entiende como una obligación en cabeza de los responsables del Tratamiento de los Datos Personales, según la cual, dichos responsables deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012. Este principio, también se lo suele denominar como *accountability*.

Tratamiento de Datos: Realizar cualquier actividad con dichos datos como: a) Capturar, almacenar y suprimir datos personales; b) Emplear, manipular, usar o procesar datos personales, para cualquier actividad legítima; c) Transmitir o transferir datos a terceros, dentro o fuera del país, para cualquier actividad legítima; d) Usar los datos para cualquier actividad relacionada con la finalidad para la cual fueron recabados o para la labor misional de la entidad que los recabó; e) Toda acción que implique la identificación del titular de los datos en donde se involucre su información personal.