Universidad de Chile
Facultad de Derecho
Programa de Magíster

LA PROTECCIÓN DE DATOS PERSONALES DE MENORES EN ESTABLECIMIENTOS ESCOLARES DE EDUCACIÓN PÚBLICA BAJO LA LEGISLACIÓN CHILENA

JUDITH MARISOL LEDEZMA CHIRINO

MEMORIA PARA OPTAR AL GRADO DE MAGISTER EN DERECHO

PROFESOR GUÍA: SALVADOR MILLALEO HERNÁNDEZ

Santiago, 2017

A **Gustavo y Judith**, mis padres, quienes me instaron a que, pase lo que pase, siempre debo seguir adelante.

A mis hermanas, **Mónica y Camila**, y a mi amado **Raimundo**, porque el camino siempre es mejor si están presentes.

A **Cayo**, mi cariño, por su apoyo y su amor.

Y a mi **Corchito**, por su silenciosa compañía en cada jornada de trabajo.

TABLA DE CONTENIDOS

CAPÍTULO SEGUNDO

OBLIGACIONES DE LOS ESTABLECIMIENTOS EDUCATIVOS PÚBLICOS Y DERECHOS DE LOS TITULARES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

CAPÍTULO TERCERO

ÁMBITO DE APLICACIÓN DE LA LEY N° 19.628 SOBRE PROTECCIÓN DE LA VIDA PRIVADA Y PRINCIPIOS DE LA PROTECCIÓN DE DATOS PERSONALES APLICADOS AL SECTOR EDUCACIÓN

CAPÍTULO CUARTO

ÓRGANOS DE CONTROL EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES EN MÉXICO, ESPAÑA Y CHILE

JURISPRUDENCIA EN MATERIA DE DATOS PERSONALES EN EL ÁMBITO DE LA EDUCACIÓN EN EL DERECHO LOCAL Y DERECHO COMPARADO

RESUMEN

La presente tesis tiene por objetivo el análisis de la situación actual de la Ley Nº 19.628 en relación a las normas que aluden a menores en su entorno escolar; básicamente se analiza los órganos públicos de educación y cómo estos cumplen con la obligación legal de proteger los datos de los educandos.

Para la realización de este análisis, se tomó en consideración la Constitución Política de la República, La Ley Nº 20.370, Ley General de Educación; la Ley Nº 19.628 sobre Protección de la Vida Privada; la Ley Nº 20.285 sobre Acceso a Información Pública, además de legislación comparada, específicamente de México y España, y la forma en que estos ordenamientos jurídicos confluyen –o discrepan- en torno a la materia analizada.

El trabajo comienza con un examen del tratamiento de los datos personales en los establecimientos de educación pública, específicamente a menores de edad, de acuerdo a la normativa legal y las competencias que se le atribuyen.

Luego, se hace referencia a las obligaciones de los establecimientos públicos de educación en lo relativo a la garantía de protección de los datos personales de los alumnos, y también una revisión de los derechos de los titulares sobre

sus datos personales; todo ello de conformidad a lo dispuesto en la Ley Nº 19.628 y la legislación mexicana y española que profusamente se han pronunciado sobre estas materias.

En tercer lugar, se contempla un análisis del ámbito de aplicación de la Ley Nº 19.628, además de la revisión detallada de los principios de la protección de datos en su dimensión nacional, como también internacional, que deben ser considerados por quienes tratan datos personales.

Finalmente, se presentan los órganos garantes de la protección de datos personales en México, España y Chile, y la forma en que estos han ido sentando jurisprudencia a través de los casos que han resuelto en materia de protección de datos de menores en centros educativos.

INTRODUCCIÓN

La sociedad en que actualmente vivimos debe compartir su espacio con ciertas circunstancias que en no pocas ocasiones la puedan afectar, entre ellas, la globalización, la tecnología y las redes sociales, las que hacen que en definitiva el actuar de los individuos que la componen se vea coartado o bien, amenazado, sobretodo en lo que respecta a su derecho a la privacidad.

Es así que la protección de datos se configura como el bastión que, en estas materias, viene a garantizar y resguardar que en el mundo en que hoy nos desenvolvemos, se ponga atención a las limitaciones a la intromisión a la vida privada de cada uno de nosotros. A este respecto, y cuando nos referimos a menores de edad, esta situación se torna más compleja, puesto que tales individuos se presentan como seres vulnerables, frágiles y aún en formación, que por ende requieren mayor resguardo en todos los aspectos de su vida, y por supuesto en lo que refiere a la protección de sus datos personales.

Es por ello que esta tesis apunta a los menores de edad como sujetos de derechos a la vida privada que requieren mayor resguardo en todos los aspectos de su vida, y a la forma en cómo el ordenamiento jurídico chileno se

hace cargo de la protección de sus datos personales, específicamente en aquellos casos en que tales antecedentes obran en poder de un órgano de la Administración del Estado, como son escuelas y liceos públicos.

Se vincula de esta manera el Derecho y la Educación, puesto que la tarea de educar se constituye como un proceso continuo y socialmente importante en que se procura la formación del conocimiento propendiéndose el respeto de los derechos y libertades de las personas; por ende, la protección de los datos personales debe comprender y sustentarse en que los alumnos desarrollen valores que permitan consolidación de su criterio personal, pretendiendo a la vez lograr una madurez cívica para actuar socialmente de manera activa, responsable y autónoma. De lo anterior se colige que los datos personales conciernen directamente a la vida personal del ser humano y que dependen en gran medida de la intervención del Estado, el que al protegerlos contribuye a garantizar prestaciones sociales a las que la ciudadanía tiene derecho, obteniendo así una sociedad más justa al evitar, a través de esta injerencia estatal, el trato discriminatorio hacia los individuos, en este caso, menores de edad.

En este contexto cabe destacar que los establecimientos educacionales – públicos y privados – ineludiblemente tratan datos personales, y no caprichosamente, sino que con un objetivo definido y determinado, pues su

finalidad se relaciona con los procedimientos de carácter administrativo que deben cumplir, amén de las obligaciones legales que les asisten. Es así que estas instituciones recogen y almacenan datos personales, entrando así en la esfera privada de sus alumnos, de los padres y apoderados, de profesores como también de profesionales de administración y servicios, inclusive de personas extrañas a la propia organización, o de personas que prestan servicios al establecimiento o que se vinculan a ella a través de proyectos de investigación.

En virtud de lo señalado, la hipótesis que se plantea en este trabajo es si en Chile la protección de datos aplicables a la educación de menores es suficiente y/o adecuada o debe ser perfeccionada con el objetivo de dar cuenta de las necesidades que emanan del principio del Interés Superior del Niño.

Por su parte, la metodología utilizada para estos efectos se traduce en el análisis detallado de la Ley Nº 19.628 sobre Protección de la Vida Privada, la Ley Nº 20.370, Ley General de Educación, además de legislación comparada, específicamente de México y España. Se analiza y coteja además la jurisprudencia del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos de México, la Agencia Española de Protección de Datos y aquella emanada del Consejo para la Transparencia, con el objetivo de verificar si las alternativas de solución legal a las que se ven enfrentados el

derecho de acceso a información pública y el derecho a protección de datos personales en el sector educación convergen, o si más bien éstas tienden a ser dispares; ello con el objetivo de establecer si existen o no brechas legales y jurídicas que nos permitan entregar una herramienta legal, eficiente y eficaz en la protección de datos y sobretodo respecto de la población más vulnerable de la sociedad, como son los niños de nuestro país.

CAPÍTULO PRIMERO

EL TRATAMIENTO DE LOS DATOS PERSONALES EN LOS ESTABLECIMIENTOS DE EDUCACIÓN PÚBLICA

1) Fenomenología del escenario escolar

La gran mayoría de los individuos han pasado por un establecimiento escolar, lugar en que han dado sus primeros pasos en la enseñanza formal. A lo largo de toda la etapa escolar – enseñanza pre- escolar, básica y media – se van desarrollando aprendizajes que le permitan sustentarse y enfrentarse a la vida adulta en forma integral. Ello por supuesto, en conjunto con el apoyo a la familia en su rol insustituible de primera educadora.

Todos estos niveles de educación permiten generar gran cantidad de antecedentes propios de cada alumno como también de su entorno familiar, social y económico; por ende, los establecimientos educativos deberán velar en todo momento por la protección de sus datos personales, los que en ocasiones pueden devenir en datos sensibles.

Ante ello la interrogante que surge es ¿cuántos y qué antecedentes obran en poder de un establecimiento educativo? Demasiados. Todos susceptibles de compartirse y darse a conocer públicamente: la Ficha formal de ingreso al establecimiento; antecedentes de discapacidad de alumnos y/o académicos o profesionales administrativos y auxiliares; datos relativos a enfermedades que puedan padecer; antecedentes respecto de alimentaciones y/o dietas especiales para algunos alumnos; antecedentes sobre actividades deportivas – recreativas; información sobre centro de alumnos; información acerca de las actividades de extensión; antecedentes respecto de la Pastoral que puedan existir en algunos establecimientos; libro de asistencia; evaluaciones académicas y evaluaciones psicopedagógicas; antecedentes sobre seguros médicos, sistemas de seguridad del establecimiento; cámaras de seguridad; entre otros.

Precisamente en atención a lo anterior, el análisis de esta tesis se centrará, fundamentalmente, en todos aquellos datos contemplados en la ficha regular de los alumnos de establecimientos de educación pública, en las obligaciones de los establecimientos, los derechos a su respecto y cómo el órgano garante debe protegerlos, en virtud del procedimiento establecido en la ley.

2) Relación entre establecimientos de educación pública y la Administración

2.a) Contexto y antecedentes históricos previos a la Constitución Política de 1980

La primera aproximación al tema de la presente tesis debe comenzar ineludiblemente por nuestra Carta Fundamental, la que en su artículo 4 señala que Chile es una República Democrática. Se colige entonces que nuestro país se sustenta en un Estado Social, donde se reconoce que las garantías fundamentales que ostentan todos y cada uno de los habitantes de la República, depende de los poderes públicos, teniendo el Estado en este escenario una responsabilidad clave en asegurar y promover una colectividad más justa que permita el desarrollo equitativo de los individuos.

Así entonces, la efectividad de estos derechos fundamentales está encomendada al Estado, el que debe presentarse como un ente fuerte, capaz de garantizar determinadas prestaciones sociales, donde los poderes públicos asumen la responsabilidad de conformar el orden social que permita a todas las personas, entre otras, el acceso a la educación. Es por ello que la educación representa una tarea de prestación social y se constituye en uno de los

primeros servicios públicos de carácter general sobre los que existe una responsabilidad de la Administración del Estado.[1]

Este derecho a la educación tiene simultáneamente el carácter de derecho individual y también de derecho social. Como ha señalado el Comité de Derechos Económicos, Sociales y Culturales de Naciones Unidas[2], *"…de muchas formas, es un derecho civil y político, ya que se sitúa en el centro de la realización plena y eficaz de esos derechos. A este respecto, el derecho a la educación es el epítome de la indivisibilidad y la interdependencia de todos los derechos humanos",*[3] y al igual que todos los derechos fundamentales, tiene un contenido esencial, puesto que no sólo es una norma programática desprovista de protección judicial - pese a la situación de no estar garantizado en nuestro país por el Recurso de Protección –, sino que se constituye en una base de aplicación directa e inmediata que impide su desconocimiento o desnaturalización.

---

[1] AGENCIA DE PROTECCIÓN DE DATOS de la Comunidad de Madrid. 2008. Protección de Datos Personales para Centros Educativos Públicos. Ed. 2008, España. Pág. 18.

[2] El Comité de Derechos Económicos, Sociales y Culturales, establecido en virtud de la resolución 1985/17, de 28 de mayo de 1985, del Consejo Económico y Social de las Naciones Unidas – ECOSOC -; es un órgano de expertos independientes para desempeñar las funciones de supervisión del Pacto Internacional de Derechos Económicos Sociales y Culturales – PIDESC - asignadas a este Consejo en la parte IV del PIDESC.

[3] NOGUEIRA ALCALÁ, H., 2008. El derecho a la educación y sus regulaciones básicas en el derecho constitucional chileno e internacional de los derechos humanos. Revista Ius et Praxis, año 14, N° 2:209-269, Chile, Pág. 210. [En línea] <http://www.scielo.cl/scielo.php?pid=S0718-00122008000200007&script=sci_arttext > [Consulta: 20 de julio de 2016]

En Chile el fundamento de este derecho radica en dos grandes fuentes: Una fuente nacional, que se materializa en la Constitución Política de Chile (1980) y en la Ley General de Educación,[4] que representa el marco para una nueva institucionalidad de la educación en Chile y que deroga la Ley Orgánica Constitucional de Enseñanza (LOCE);[5] y las fuentes internacionales, como los Tratados Internacionales firmados por Chile con implicaciones en la materia contenidos específicamente en la Convención sobre los Derechos del Niño (1959 y 1989) y la Declaración Universal de los Derechos Humanos (1948).[6]

En cuanto a la evolución del establecimiento e institucionalización de este derecho, cabe indicar que la Ley General de Instrucción Primaria se promulgó el 24 de noviembre de 1860, asumiendo el Estado por primera vez un rol en la dirección principal de la educación primaria, garantizando su gratuidad, clasificando las escuelas en elementales y superiores, y haciéndose cargo del gasto fiscal estatal y municipal. Sin perjuicio de las acciones realizadas, a fines del siglo XIX y principios del siglo XX, la gratuidad de la educación reveló su

[4] DECRETO CON FUERZA DE LEY Nº 2, que fija texto refundido, coordinado y sistematizado de la Ley N° º 20.370 con las normas no derogadas del Decreto con Fuerza de Ley Nº 1, de 2005. Fecha de promulgación: 16 de diciembre de 2009. Santiago, Chile. [En línea] < http://www.leychile.cl/Navegar?idNorma=1014974> [Consulta: 20 de mayo de 2016]

[5] La derogación refiere a la educación general básica y media, pues se mantienen la normativa respecto a la educación superior, estableciendo principios y obligaciones, y promoviendo cambios en la manera en que los niños de nuestro país serán educados.

[6] REDONDO, J; ALMONACID, C; INZUNZA, J; MENA, P.; DE LA FUENTE, L., 2007. El derecho a la educación en Chile. Colección Libros FLAPE, Chile. Pág. 10. [En línea] < http://www.opech.cl/bibliografico/Doc_Financiamiento/08Chile_Derecho.pdf > [Consulta: 24 de mayo de 2016]

insuficiencia dadas las altas tasas de analfabetismo y el alto número de niños y niñas que quedaban fuera del sistema educativo.[7]

Ante la realidad de la época y las nuevas necesidades económicas y culturales del país, en 1920 surge la Ley de Instrucción Primaria Obligatoria,[8] que dispuso que la educación primaria de provisión estatal y municipal es gratuita y obligatoria al menos por cuatro años, obligación que recae sobre los padres, guardadores o personas a cargo de los menores. La educación primaria estaba a cargo del Ministerio de Instrucción Pública, delegando funciones de vigilancia y dirección inmediata en el Consejo de Educación Primaria, cuyas funciones eran de apoyo y de carácter administrativo.

Posteriormente, a partir de la Constitución de 1925 se observa en Chile el nacimiento del Estado liberal,[9] docente, desarrollista y populista, que continuó la estrategia mercantil de las compañías europeas, con un populismo asistencial y una política anti-imperialista, que subordinó a todos los movimientos sociales bajo la clase política civil.[10]

[7] Ibid, Pág. 12.

[8] 26 de agosto de 1920.

[9] Considerado también como un Estado empresarial.

[10] REDONDO, J; ALMONACID, C; INZUNZA, J; MENA, P.; DE LA FUENTE, L., Op. Cit. Pág. 15.

Fue en los gobiernos radicales (1938-1952) cuando el Estado priorizó la protección y los cuidados básicos de la población, asignando mayores recursos económicos. Se comienza con la experimentación pedagógica en las escuelas primarias, surgiendo el Liceo Experimental Manuel de Salas en el año 1932, los Liceos Experimentales del Movimiento de Renovación Educacional, y se instala la concepción del Estado docente y la responsabilidad preferente del Estado por la educación pública. Con ello emerge la necesidad de elaborar una ley orgánica de educación pública que coordinara las diferentes ramas de la enseñanza y permitiera establecer un control estatal sobre los establecimientos privados.

No obstante estas ideas, y aun cuando la cobertura escolar aumentó en la década de los años 30, los gobiernos de la época no lograron realizar cambios profundos en la estructura ni en la orientación del sistema escolar, pues las iniciativas en educación carecieron de profundidad y de consenso político.

Ya en los años 40 se inicia una fase de medidas y reformas parciales, que implicaron la puesta en marcha de establecimientos experimentales caracterizados por la estrecha relación de teoría y práctica, la vivencia de una gestión democrática, la promoción de proyectos institucionales, la interdisciplinariedad, el liderazgo docente y el contacto con la comunidad externa.

Luego, en el año 1961 se establecieron las Bases Generales para el Planeamiento de la Educación Chilena, que reconoce la creciente relación entre desarrollo económico y educación y las deficiencias que el sistema educativo tenía para resolver esta vinculación, lo que condujo a que en 1963 se realizara un análisis de todo el sistema educativo – niveles y tipos –, estableciéndose la necesidad de unidad y continuidad de los servicios escolares públicos y privados, integración de todo el territorio nacional, desarrollo de la educación regular, complementaria y de adultos, y vinculación del desarrollo social, económico y educacional.

A fines de 1964 el presidente Eduardo Frei Montalva inicia una amplia planificación de una reforma profunda y gradual de la educación chilena, cuyo objetivo fue una mayor cobertura y diversificación del sistema escolar, la mejora de la calidad y la racionalización de la administración a través de planes de corto y largo plazo, la responsabilidad socio-cultural de la Educación, la formación y la educación como proceso para toda la vida, lo que implicó cambios y compromisos de acción educadora más allá de la de la propia comunidad educativa que conllevaron a centrarse en el desarrollo armónico e integral de la personalidad y de preparación para la vida del trabajo.[11]

[11] Ibid, Pág. 19.

Durante el gobierno de Salvador Allende (1970-1973), con la realización de congresos locales y provinciales, nace el Proyecto Escuela Nacional Unificada (ENU)[12] cuyo objetivo fue generar un auténtico Sistema Nacional de Educación que permitiera la igualdad de oportunidades y favoreciera el pleno desarrollo de las capacidades y singularidades humanas, además de la integración social. Luego con el golpe militar del año 1973 se privatizó la educación, se da lugar a la educación privada subvencionada – financiada por el Fisco –, a la instalación de un sistema híbrido de conducción administrativa municipal y orientación técnica del Ministerio de Educación, a la dismunición del financiamiento en educación, lo que conllevó a una progresiva desvalorización de la formación docente.[13]

[12] La Escuela Nacional Unificada (ENU) fue un proyecto de transformación integral de la educación chilena, impulsado por el gobierno de Salvador Allende tras un largo debate durante 1971 que involucró a diversos actores como docentes, estudiantes, padres y organizaciones sociales. El balance que se hizo por entonces era que la educación debía ser permanente (desde el nivel preescolar y durante toda la vida), democrática, participativa, pluralista y acorde con las necesidades económicas del país. El documento que se elaboró incluía la creación de amplios mecanismos de participación, la integración de los distintos niveles en un solo sistema y la eliminación de las diferencias entre la enseñanza técnica y humanista. Sin embargo, a pesar del empeño puesto por el gobierno, el proyecto generó muchas resistencias al sospecharse que detrás de él existía el propósito de instalar una educación ideologizante de tipo socialista. De esta manera, en 1973 se postergó su implementación, al no obtener el apoyo político de la oposición.

[13] REDONDO, J; ALMONACID, C; INZUNZA, J; MENA, P.; DE LA FUENTE, L., Op, Cit. Pág. 19.

2.b) Antecedentes históricos posteriores a la Constitución Política de 1980

La Constitución Política de 1980 responde, como todo cuerpo legal, a su contexto político e histórico; surge como una necesidad para el gobierno de la época, que hasta el momento había gobernado sólo a través de Decretos Leyes. Esta Constitución sostiene en términos generales un régimen presidencialista, un rol subsidiario del Estado, una fuerte protección de las garantías individuales en cuanto al ámbito económico y derechos de propiedad, además de un Estado unitario y dividido en trece regiones.[14]

En lo que respecta al derecho a la educación en Chile, éste se encuentra consagrado en el artículo 19 Nº 10, Capítulo III de nuestra Carta Fundamental: *"De los Derechos y Deberes Constitucionales"*, sosteniéndose que la educación tiene por objeto el pleno desarrollo de la persona en las distintas etapas de su vida, siendo los padres los primeros responsables –con derechos y deberes – de educar a sus hijos. El rol que corresponde al Estado es el de otorgar especial protección al ejercicio de este derecho, financiando un sistema gratuito

[14] Quince regiones en la actualidad. Ley N° 20.174 que crea la XIV Región de Los Ríos y la Provincia de Ranco en su territorio, Ministerio del Interior; Subsecretaría del Interior; fecha de publicación: 05 de abril de 2007; y Ley N° 20.175 que crea la XV Región de Arica y Parinacota y la Provincia del Tamarugal en la Región de Tarapacá, Ministerio del Interior; Subsecretaría del Interior, fecha de publicación: 11 de abril de 2007.

que asegure el acceso a toda la población a la educación básica y media, promover la educación parvularia, fomentar el desarrollo de la educación en todos sus niveles, estimular la investigación científica y tecnológica, la creación artística y la protección e incremento del patrimonio cultural de la Nación.

Una de las implicancias más importantes del precepto constitucional citado es que el Estado cumple un rol subsidiario en educación, asumiendo constitucionalmente su imposibilidad de hacerse cargo de la tarea educativa en su totalidad, pasando a desempeñar un rol complementario y privilegiando a los padres como principales responsables de esta labor. A su vez incorpora a la comunidad general en esta misión,[15] asumiendo que los establecimientos escolares son formas de organización intermedia de la sociedad que actúan bajo el principio de la libertad de enseñanza.

Importante es destacar que el derecho a la educación se complementó y operacionalizó dentro de la legislación chilena con la Ley N°18.962, Ley Orgánica Constitucional de Enseñanza - LOCE -, publicada el 10 de marzo de 1990, actualmente derogada por la Ley General de Educación, Ley Nº 20.370. La referida LOCE, estableció los requisitos para los niveles de enseñanza

[15] Artículo 11 de la Constitución Política que guarda estrecha y directa relación con el citado artículo 10 de mismo cuerpo legal, al hacer referencia a la participación privilegiada de la comunidad en la tarea educativa.

básica y medio, imponiendo al Estado la tarea de velar por su cumplimiento y otorgándole la facultad de dar el reconocimiento oficial a los establecimientos educativos, respetando siempre el principio de libertad de enseñanza.

Los principales ejes que presentaba la LOCE eran:

a) Objetivos generales y características de cada nivel de enseñanza: Educación parvularia; Enseñanza básica; Enseñanza media.

b) Procesos de selección.

c) Currículum.

d) Evaluación.

e) Sostenedor.

f) Requisitos para abrir establecimientos.

g) Educación superior.

h) Consejo Superior de Educación.[16]

En cuanto a la Ley General de Educación, Ley N° 20.370 – LGE - , su origen viene dado por el surgimiento del Consejo Asesor Presidencial para la Educación Superior que recogió las demandas emanadas de la movilización estudiantil secundaria del año 2006,[17] que intentó dar respuesta a estas

[16] REDONDO, J; ALMONACID, C; INZUNZA, J; MENA, P.; DE LA FUENTE, L., Op. Cit. Pág. 26.

[17] Las demandas iniciales son reivindicaciones económicas puntuales pero - a poco andar – se cuestiona el sistema educativo de un modo global. Los secundarios declaran la educación en crisis, cuyo fundamento se erige en la desigualdad del sistema educativo, puesto que éste

demandas, planteándose una serie de propuestas de reforma a la LOCE que, finalmente, se articulan en un proyecto de ley. De esta manera la LGE se constituyó como un significativo avance respecto de la LOCE, específicamente en los siguientes puntos clave.

- Constituye una ley en democracia que buscó la derogación de la LOCE.
- Incorpora y enfatiza los principios de calidad y equidad educativa.
- Refuerza el concepto de Comunidad Educativa con deberes y derechos para sus integrantes: Centros de Estudiantes, Centros de Padres y Apoderados, Consejos de Profesores y Consejos Escolares.
- Establece requisitos más exigentes para incorporarse como sostenedor al sistema educativo y mantenerse en éste.
- Los sostenedores sólo podrán ser personas jurídicas, poseer giro único, y los que reciban recursos del Estado deberán rendir cuenta pública de los mismos.

En cuanto al control de la calidad de la educación, se crea un Sistema Nacional de Aseguramiento de la Calidad de la Educación, que deberá

---

entrega a los estudiantes una educación de calidad desigual, fuertemente relacionada con los ingresos familiares del educando: educación privada para unos y municipal para otros, lo que se expresa y refleja en los resultados disímiles obtenidos en la PSU, prueba que define el ingreso a la universidad. Para los secundarios las causas que originan esta desigualdad estarían en el ordenamiento jurídico e institucional del sistema educacional, el que ubican en: (i) La ley que regula al sistema educativo (la LOCE); (ii) La ideología neoliberal que justifica y sostiene el actual orden jurídico mercantil del sistema educativo; y (iii) La administración de la educación de propiedad del estado por los municipios

encargarse de mantener los estándares de calidad a través de cuatro instituciones:

i.) Ministerio de Educación: Propone las bases curriculares, programas de estudio y estándares de calidad, y da apoyo a los establecimientos para su cumplimiento.

ii) Consejo Nacional de Educación: Nueva institución creada por la LGE, que aprueba las bases, planes y estándares de calidad concebidos por el Ministerio. En el caso de la evaluación de desempeño de los establecimientos, esta se realizará a partir de estándares indicativos de desempeño que serán propuestos por el Ministerio y aprobados por el Consejo Nacional de Educación; y tiene por finalidad fortalecer las capacidades institucionales y de autoevaluación de los establecimientos y facilitando con ello el desarrollo de planes de mejora.

iii) Agencia de Calidad de la Educación: Nueva institución que evalúa e informa sobre la calidad de los establecimientos educacionales, siendo el órgano encargado de resguardar y asegurar el cumplimiento de los estándares de calidad de la educación que defina el Ministerio de Educación, debiendo determinar aquellos estándares de calidad académica comunes a todos los establecimientos educacionales, que tendrán que ser visados por el nuevo Consejo Nacional de Educación y que permitirá a las familias exigir igualdad de condiciones de calidad para todos los establecimientos (calidad

docente, recursos e infraestructura educacional, cumplimiento curricular, etc.), además tiene la responsabilidad de desarrollar el sistema de medición de la calidad de los aprendizajes de los alumnos y de evaluación del desempeño de los establecimientos.

iv) Superintendencia de Educación: Nueva institución encargada de fiscalizar que los establecimientos educacionales cumplan con las normas educacionales y las cuentas públicas, cuando corresponda, debiendo regular y controlar el uso de los recursos fiscales, amén de fiscalizar y auditar la rendición de cuentas de los establecimientos y sus sostenedores. El fin último de este nuevo órgano es resguardar que los recursos que el Estado aporta sean utilizados en beneficio de una educación de calidad y no desviados hacia otros fines, pues en tal caso, frente al incumplimiento de esta obligación la Superintendencia tiene las competencias necesarias para establecer sanciones específicas.[18]

Finalmente, dispone este cuerpo legal que:

- Las familias pueden conocer el proyecto educativo del establecimiento.
- Se mantiene la norma sobre protección de embarazo y maternidad.

[18] BIBLIOTECA DEL CONGRESO NACIONAL. 2013. Chile. Guía legal sobre Ley General de Educación. Detalla las novedades que trae la Ley General de Educación, que establece un marco institucional para la educación escolar. [En línea] <http://www.bcn.cl/leyfacil/recurso/ley-general-de-educacion> [Consulta: 23 de noviembre de 2016]

- Se incorporan normas que fortalecen la protección de los estudiantes en relación a la cancelación de la matrícula y sanciones por el no pago de compromisos de los padres.
- Se prohíben las expulsiones por rendimiento académico entre pre kinder y sexto básico, y
- Se establece el derecho de los estudiantes a repetir un curso en la enseñanza básica y uno de la enseñanza media en un mismo establecimiento.[19]

2.c) Estructura y funcionamiento del Sistema Educativo Escolar en Chile (educación básica y media)

A este respecto señalar que en la actualidad, en sus distintas modalidades, la estructura y funcionamiento del sistema es provista a través de un sistema mixto, en el que participan los sectores públicos y privados, tanto en la producción como en el financiamiento de la actividad. La educación financiada por el sector público tiene carácter descentralizado y opera con productores

[19] MINISTERIO DE EDUCACIÓN. s.a. Ejes claves del proyecto de ley general de educación. Chile. [En línea] <http://portales.mineduc.cl/usuarios/formacion_tecnica/File/2011/ESTUDIOS/Ejes_claves_proyecto_LGE.pdf> [Consulta: 23 de julio de 2016]

privados y municipales, lo que permite la existencia de tres tipos de colegios: los municipales, los privados subvencionados y los privados pagados.[20]

En la materia que nos ocupa en la presente tesis, se abarcará lo relativo a colegios públicos y aquellos privados subvencionados, siendo plausible indicar que éstos son, en general, gratuitos y se financian principalmente a través de aportes fiscales, mientras que establecimientos particulares pagados son financiados a través de los cobros de matrícula.

Respecto al financiamiento municipal, éste es realizado a través de un esquema de subvención educacional o subsidio por estudiante, el que debe cubrir los gastos de operación y de capital de los establecimientos. El propósito de esta forma de aporte es promover la competencia entre las escuelas bajo financiamiento fiscal - tanto públicas como privadas - para atraer y retener alumnos al vincular y generar dependencia entre el ingreso de los establecimientos y la elección que efectúen los alumnos y sus familias, donde el objetivo final buscado es promover una mayor eficiencia y calidad de los servicios educacionales entregados por dichos establecimientos.[21]

[20] Existen también las corporaciones de administración delegada que corresponde a gremios empresariales o corporaciones privadas que administran liceos técnicos-profesionales, con financiamiento público vía convenio.

[21] AEDO, C., s.a. Educación en Chile: Evaluación y Recomendaciones de Política. Chile. Pág. 2. [En línea] <http://fen.uahurtado.cl/wp-content/uploads/2010/07/inv125.pdf **>** [Consulta: 10 de agosto de 2016]

En cuanto al control, ambos tipos de establecimientos están sujetos a controles de parte del nivel central; sin embargo, la penalización tiene impactos diferentes, pues en el sector privado subvencionado la consecuencia de infringir la regulación se traduce en una penalización financiera importante; mientras que en el sector municipal, tal infracción constituye un mayor déficit municipal en educación, con la consiguiente presión para que el nivel central - Ministerio de Educación o Ministerio del Interior - efectúe transferencias hacia la municipalidad para solventar dicho déficit.

Según Cristian Aedo, uno de los factores relevantes y que tiene incidencia en el esfuerzo realizado para lograr una gestión eficiente en la administración de los establecimientos, es que la asignación de los recursos se efectúa tomando en consideración los resultados obtenidos, lo que se traduce en que, por una parte, los sostenedores de los colegios privados subvencionados deben poner todo su esfuerzo para obtener buenos resultados con el fin de captar matrículas y mantener una buena asistencia de los alumnos a la escuela; y por la otra, que si los sostenedores de los colegios municipales no cubren sus gastos con los ingresos por subvención reciben transferencias municipales - subvención municipal - las que en muchas entidades edilicias son financiadas finalmente por el nivel central, con ingresos extra-subvención que generan una asignación de los recursos la que no depende de los resultados educacionales obtenidos, y

que finalmente afecta de forma negativa a la eficiencia de la gestión en estos establecimientos.

En lo relativo a los actores y la gestión educacional del sistema organizacional de los establecimientos, en aquellos de carácter particular subvencionado se observa un trabajo en equipo entre el Director del colegio y el propietario (sostenedor), quien tiene una participación directa y permanente; a diferencia de los colegios municipales en los que se observa un diferente grado de delegación de autoridad, dependiendo de la persona que se encuentre a cargo de la Corporación.

En segundo lugar, en los colegios privados subvencionados la contratación de personal se realiza de forma conjunta entre el sostenedor y el Director de la escuela, lo que permite que el Director tenga un mayor control sobre el recurso humano. Para el caso municipal, en general, la contratación de docentes la efectúa la Corporación o la Dirección de Administración de Educación Municipal – DAEM - y sólo en ocasiones se solicita la opinión del Director.

En tercer término, los niveles salariales establecidos por los colegios privados subvencionados se determinan, por lo general, a través de una negociación colectiva y sobre la base del Estatuto Docente, donde los criterios utilizados para tal determinación están en función de su experiencia,

capacitación y desempeño en el colegio. Por su parte, los salarios en el sector municipal se establecen también en función al Estatuto Docente, pero en este caso los criterios para la determinación del nivel salarial son rígidos y están establecidos en función de la experiencia, capacitación y nivel de responsabilidad; por ende es dable concluir que en este caso, el tipo de desempeño educacional realizado no influye en el sueldo recibido.[22]

3) Administración Educacional

En el campo propio de la administración de la educación, se observa que ella, sin dejar de formar parte y de informarse de la Administración en general, tiene su propia naturaleza y persigue sus propósitos específicos: la administración de los sistemas educativos, la administración del desarrollo educativo, la función que asume, la responsabilidad de asegurar el cumplimiento de las políticas educativas que deben necesariamente ser formuladas, aprobadas, planificadas, ejecutadas y evaluadas en un proceso integrado en cual siempre y ejerciendo un papel muy significativo, está presente la administración educativa. De lo anterior es posible desprender que desde un punto de vista denominado "*funcional*", la administración educativa tiene a su cargo la implementación de las políticas educativas; lugar desde donde

[22] Ibid, Pág. 25.

proviene la contribución final de la función administrativa y específicamente la administración de la educación. Sin embargo, existe también otro enfoque, denominado "*institucional*", que toma en cuenta a la administración educativa principalmente como el conjunto de las estructuras organizacionales que deben asegurar la prestación de los servicios educativos a la población, caso en el cual la consideración es mayormente instrumental, disponiendo de un campo de análisis mucho más concreto, que corresponde al de la superestructura que administra el sistema educativo propiamente dicho.

Así, la administración educativa que se refiere a la gestión de las instituciones, públicas o privadas, que producen servicios educativos y que va a la par de nuevas concepciones, apuntan hacia la administración social de los servicios educativos a la escala comunal que involucra a las instituciones, programas y actividades educativas locales, y que al mismo tiempo se articula con la administración gubernamental propiamente dicha; en todas estas formas y niveles de la administración educativa, la finalidad última es la misma, aun cuando la naturaleza y los propósitos específicos varíen.[23]

[23] MALPICA, C., 1980. Administración de la Educación y sus relaciones con la planificación y con la investigación. *R*ae Eugène-Delacroix, 75016 Paris LA, Instituto Nacional de Planeamiento de la Educación. (creado por la Unesco), Perú. Pág. 7 [En Línea]< http://unesdoc.unesco.org/images/0007/000701/070174so.pdf > [Consulta: 06 de julio de 2016]

Atendido lo señalado precedentemente, es plausible sostener que el vínculo entre educación pública y Administración viene dado por la prioridad que el Estado debe otorgarle a aquella. En este sentido conviene recordar que lo que define a la educación pública no es que sea financiada con recursos del Estado; en efecto, diversos Estados financian establecimientos privados entregándoles diferentes tipos de subsidios - dinero, recursos humanos, o exención de impuestos - , y aunque el Estado hace ciertas exigencias a los proveedores privados a cambio de los recursos que les entrega, no toma, sin embargo, el control de la administración de dichos establecimientos para decidir sobre las cuestiones críticas de la gestión educacional: los establecimientos privados continúan sirviendo primeramente los objetivos, intereses y orientaciones de sus propietarios.[24]

En consecuencia, mientras que para los establecimientos privados cooperar con el bien común es una opción entre varias, para la educación pública es su obligación esencial, puesto que precisamente en ello se basa la necesidad de que el Estado tenga con la educación pública un trato preferente con visión más social y más aun considerando el volumen y la complejidad de los datos personales y/o sensibles que les corresponde y compete administrar y respecto

[24] BELLEI, C., 2011. La educación pública que Chile necesita. Revista “El Chile que se viene”, R. Lagos y O. Landerretche, Ed., F. Democracia y Desarrollo y Ed. Catalonia, Chile. Pág. 6. [En línea] <http://www.ciae.uchile.cl/download.php?file=noticias/BELLEI%20-Chile2030.pdf. > [Consulta: 06 de julio de 2016]

de los cuales necesariamente debe disponer de las acciones pertinentes que garanticen efectiva seguridad en el tratamiento.

4) Las instituciones educacionales públicas como cedentes y cesionarios de información personal: la publicidad en el ámbito educativo

Desde el momento en que los padres y/o apoderados solicitan el ingreso de sus hijos en un colegio hasta el momento en que éstos abandonan, los establecimientos educacionales que los acogen se convierten en receptores de sus datos de carácter personal como también de aquellos de carácter sensibles, que pueden afectar su imagen, su honor, su intimidad personal, su pertenencia a minorías étnicas, su religión, su salud en algunos casos e inclusive sus capacidades físicas e intelectuales.

En el caso de los colegios, al disponer de todos estos antecedentes que afectan al menor y consecuentemente a su entorno familiar, el tratamiento y/o cesión de datos de carácter personal debe contar con el consentimiento de sus padres y /o apoderados. Por tanto, si el colegio carece del expreso consentimiento por parte de los padres, apoderados o quien tenga al menor a su cuidado para el tratamiento de los datos personales, éste no podrá realizar,

por ejemplo, ningún traslado de expediente de alumnos a otro colegio, como tampoco podrá entregarse datos o informes a facultativos médicos externos, a empresas de transportes, a casas comerciales, ni tampoco podrá realizarse transferencias internacionales de datos para intercambio internacional de alumnos.[25]

En el ámbito educativo, la Ley N° 20.370 establece en términos generales los lineamientos fundantes al regular los derechos y deberes de los integrantes de la comunidad educativa, además de requisitos para cada nivel educacional y los requisitos y proceso para reconocimiento oficial de instituciones educativas. Sin perjuicio de ello, del examen de la norma citada no es posible encontrar protección o garantías expresas relativas a datos de niños, niñas o adolescentes en poder de los centros educativos, lo que consecuentemente dificulta la forma en que los derechos de los titulares de datos serán amparados.

El artículo 3 letra f) de la Ley Nº 20.370 dispone que el sistema educativo chileno se construye sobre la base de los derechos garantizados en la Constitución, así como en los tratados internacionales ratificados por Chile y

[25] EQUAL PROTECCIÓN DE DATOS. 2014. La implantación de la LOPD en los colegios. España. [En línea] <https://equalprotecciondedatos.com/lopd-en-los-colegios/ > [Consulta: 11 de julio de 2016]

que se encuentren vigentes y, en especial, del derecho a la educación y la libertad de enseñanza. Se inspira, además, en el principio de Responsabilidad, donde todos los actores del proceso educativo deben cumplir sus deberes y rendir cuenta pública cuando corresponda. Por su parte, el artículo 29 Nº 2, letra d) de la misma ley, dispone que la educación básica tendrá como objetivos generales, sin que esto implique que cada objetivo sea necesariamente una asignatura, que los educandos desarrollen los conocimientos, habilidades y actitudes que les permitan acceder a información y comunicarse usando las tecnologías de la información y la comunicación en forma reflexiva y eficaz.

De las normas transcritas resulta poco claro la obligación y menos aún la protección que brinda el ordenamiento jurídico a los menores en el ámbito de la protección de sus datos personales, limitando su acción a que el establecimiento debe cumplir con sus obligaciones escolares (básicos y secundarios) y rendir cuenta pública en los casos que corresponda, sin hacer referencia si es posible acceder o no a documentación de los menores y/o personal docente o administrativo del establecimiento. Misma situación respecto del objetivo de la educación básica de permitirle a los alumnos acceder a información usando las tecnologías de la información, puesto que no existe una norma que complemente este cuerpo legal, que regule directamente la forma de acceder a tal información, las medidas de seguridad asociadas, pues como sabemos en comunicaciones electrónicas, por redes sociales, es posible que

tanto niños, niñas y adolescentes entreguen información para acceder a juegos, plataformas virtuales, comercio, etc., no existiendo por tanto, garantías para que sus derechos a la privacidad sean amparados.

Nuestra Ley Nº 19.628 [26] en su artículo 2 dispone una serie de conceptos de relevancia para entender estas materias. El primero de ellos, y que da pie inicial para analizar su normativa es la letra f), que a su tenor señala: *"Datos de carácter personal o datos personales, los relativos a cualquier información concernientes a personas naturales, identificadas o identificables".* De este precepto legal es posible inferir, que la ley en comento, aun cuando no refiere expresamente a niñas, niños o adolescentes, los incluye al considerarlos personas naturales; en consecuencia, la ley es posible aplicarla a su respecto.

Por su parte, el mismo artículo 2 letra c) establece como *"comunicación o transmisión de datos: dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas.";* en este sentido, se colige que quien realiza actos de cesión es el responsable de un registro o banco de datos, y es a quien le competen las decisiones relacionadas con el tratamientos de datos de carácter personal, por ello toma especialmente relevancia el asunto en atención a que existen diversos terceros

[26] Ley N° 19.628 sobre Protección de la Vida Privada, Ministerio Secretaría General de la Presidencia, fecha de publicación: 28 de agosto de 1999.

que eventualmente pudieran tener interés en los datos personales, los que, ejerciendo su derecho de acceso a información a la institución del sistema educacional, podrían acceder directamente a tales antecedentes, más aún si la ley en comento establece que cuando existan datos provenientes de fuentes accesibles al público, ésta no requiere de autorización para su tratamiento; sin embargo, importante es destacar que ello no significa que el titular del banco de datos no deba cumplir con el deber de informar al afectado que se está tratando información que le afecta, puesto que al ser la comunicación de datos una operación de tratamiento de los mismos, es de suyo sostener que en tales casos debería informarse al interesado dichas operaciones, indicando a la persona a la cual se transmiten, el fundamento legal de la transmisión y la finalidad para la cual son requeridos.[27]

Para el adecuado tratamiento de los datos personales que dispone el establecimiento educacional, será menester la celebración de contratos de confidencialidad que deben ser suscritos por el colegio y su personal, contratos que no sólo deben suscribirse con el personal docente, sino también con el personal administrativo, para de esta manera obligarlos a guardar reserva respecto de los datos de que conozcan y sean derivados de sus funciones. Por su parte, atendida la información que se maneja en colegios de educación

[27] DONOSO, L., 2009. El tratamiento de datos personales en el sector de la educación. Expansiva UDP. En Foco 136, ISSN 0717-9987, Chile. Pág. 22. [En línea] < http://www.expansiva.cl/media/en_foco/documentos/15042009150219.pdf > [Consulta: 11 de julio de 2016]

primaria y secundaria, será obligatorio inventariar soportes informáticos de que dispongan, realizar copias que respalden la información respectiva y mantener medidas que permitan la recuperación de los datos de carácter personal tanto digitales como en soporte papel.

En otro orden de ideas, en cuanto a la publicidad de las resoluciones administrativas, debe tenerse en consideración que éstas pudieran contener información personal, caso en que cual conviene destacar que son muchos los procedimientos de concurrencia competitiva en el ámbito educativo; por ejemplo, la admisión de nuevos alumnos a los distintos establecimientos educacionales, convocatorias de becas y beneficios, entre otros, que se constituyen en procedimientos en los que se ven involucrados diversos actores y en los que se maneja gran cantidad de antecedentes personales de los mismos; debiendo en tales casos ponderarse si la información puede o no ser entregada.[28]

Específicamente en lo relativo a datos sensibles, la Ley N° 19.628 prevé en su artículo 10 que "*no pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que*

[28] AGENCIA DE PROTECCIÓN DE DATOS de la Comunidad de Madrid, Op. Cit. 68.

correspondan a sus titulares." Y en este sentido, debe tenerse presente que además la ley en su artículo 11 dispone que "*el responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños*"; por ende es plausible sostener que la ley propende a un cuidado especial respecto de estos datos.

A este respecto, la profesora Lorena Donoso sostiene que la problemática resulta compleja, puesto que será necesario analizar caso a caso si existe fundamento legal para la comunicación de este tipo de datos. Señala que, tratándose de las solicitudes de información al Ministerio de Educación, para las fiscalizaciones del funcionamiento de los establecimientos educacionales, por ejemplo, o para la entrega de recursos por concepto de subvenciones, rige lo dispuesto en el artículo 15 de la ley en comento,[29] en el sentido de que no podrá entorpecerse las necesidades de información de dicho organismo bajo pretexto de requerirse información, por verse el derecho de información, modificación, cancelación y bloqueo limitado en este caso.[30]

---

[29] *"No obstante lo dispuesto en este Título, no podrá solicitarse información, modificación, cancelación o bloqueo de datos personales cuando ello impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido, o afecte la reserva o secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la Nación o el interés nacional.*
Tampoco podrá pedirse la modificación, cancelación o bloqueo de datos personales almacenados por mandato legal, fuera de los casos contemplados en la ley respectiva". Artículo 15, Ley N° 19.628.

[30] DONOSO, Op. Cit. Pág. 23.

En términos generales, se habla de cesión de datos de establecimientos educacionales cuando se refieren a datos del educando (alumnos) – punto central de esta tesis -; sin embargo y desde la otra vereda, es importante destacar que estos centros educativos no sólo tratan datos de aquellos, sino también de docentes, administrativos, personal auxiliar e inclusive de padres y apoderados. En este escenario y tomando en consideración la vasta legislación española valga señalar que ésta dispone que, la primera obligación al recabar un dato personal es proceder a la declaración del registro a través de una disposición de carácter general, publicar la disposición e inscribir los ficheros en los registros correspondientes.[31] Siguiendo esta lógica, la administración educativa debe respetar todos los principios y derechos de protección de datos, entre ellos el de calidad, esto es que la finalidad del tratamiento sea legítima y que esté dentro de las competencias del órgano administrativo y que en todos estos casos los datos que se recaben sean adecuados, pertinentes y no excesivos en atención al cumplimiento de la finalidad; en consecuencia, no será posible recabar antecedentes personales de los alumnos en aquellos casos en que no diga relación con la finalidad pre-establecida. Así, en aquellos casos en que los alumnos entreguen sus datos para solicitar cupo para beca estudiantil,

---

[31] TRONCOSO, A., 2006. La publicación de datos de profesores y alumnos y la privacidad personal. Acerca de la protección de datos en las Universidades. Revista de Derecho Político, Num. 67, España. Pág. 118. [En línea] < http://revistas.uned.es/index.php/derechopolitico/article/view/8999/8592 > [Consulta: 25 de julio de 2016]

éstos no pueden ser utilizados para una finalidad distinta e incompatible, es decir, no podrían ser utilizados, por ejemplo, invitaciones para actividades extraprogramáticas.

Un aspecto a considerar en este punto es la publicación de resultados de procedimientos concursales en alguna página web del respectivo servicio, que se traduce básicamente en una comunicación de datos a terceras personas. La ley española de Régimen Jurídico de las Administraciones Públicas y Procedimiento Administrativo Común, Ley 30/1992 de 26 de noviembre[32] dispone que la notificación del acto administrativo, cuando se trate de actos integrantes de un procedimiento selectivo o de concurrencia competitiva de cualquier tipo, se realizará mediante la publicación del acto. Por ende, la publicación de los listados de postulantes de un proceso de este tipo no es potestativa sino que es obligatoria en cumplimiento del principio de publicidad que rige todas las convocatorias de pruebas selectivas y de acuerdo a las bases de las mismas; de esta manera, las bases de la convocatoria deberán indicar el tablón de anuncios o medio de comunicación donde se vayan a

[32] Última actualización, publicada el 17/09/2014, en vigor a partir del 18/09/2014. El Boletín Oficial del Estado publica el 02 de octubre de 2015 que las dos normas básicas sobre las que se estructurará el régimen de las Administraciones Públicas a partir de septiembre de 2016 son la Ley 39/2015 del Procedimiento Administrativo Común de las Administraciones Públicas **-** de 1 de octubre - **,** y la Ley 40/2015, de Régimen Jurídico del Sector Público**,** de misma fecha**;** los que se constituyen en los cuerpos legales que, a contar de la fecha indicada, provocarán la derogación de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento administrativo Común, con la que España ha venido funcionando los últimos 24 años.

realizar las sucesivas publicaciones, careciendo de validez las que se publiquen en lugares distintos; publicación que también podrá ser en sitios web.

Dispone el ordenamiento jurídico español que la finalidad de la publicación de cualquier listado con datos personales de los integrantes de un proceso selectivo es, por una parte, servir de notificación del acto administrativo al interesado y por la otra, garantizar el principio de publicidad de un procedimiento de concurrencia competitiva y transparencia de la actividad administrativa. En virtud de este procedimiento se permite que la comunidad conozca el resultado final, y en su caso, pueda reclamar el expediente para su revisión como también para que proceda a su impugnación, razón por la que en la ley española es legítimo publicar la resolución del procedimiento en tablones de anuncios, en boletines oficiales[33] y en páginas web, pues la publicidad de la resolución supone una cesión de datos a terceras personas, no siendo

[33] A este respecto señalar que la Constitución española dispone en su artículo 9.3 que «*La Constitución garantiza […] la publicidad de las normas*», por tanto es un imperativo legal la publicación de las normas, lo que se canaliza a través de los distintos boletines oficiales, el BOE en su caso.
El Boletín Oficial del Estado (BOE) es el Diario Oficial del Estado español. De acuerdo con el Real Decreto 181/2008, de 8 de febrero, el *BOE* es el Diario Oficial del Estado español, constituyéndose como el medio de publicación de las leyes, disposiciones y actos de inserción obligatoria, que contiene además las leyes aprobadas por las Cortes Generales, las disposiciones emanadas del Gobierno de España y las disposiciones generales de las comunidades autónomas. Su edición, impresión, publicación y difusión está encomendada, en régimen de descentralización funcional, a la Agencia Estatal Boletín Oficial del Estado.

necesario el consentimiento del interesado, en atención a que existe una habilitación legal para ello, precisamente la Ley 30/1992 antes citada.[34]

Señala el profesor Troncoso Reigada que no obstante lo anterior, si bien se presenta como legítima la publicación de los resultados finales de los procedimientos selectivos o de concurrencia competitiva en los boletines oficiales o en la web, resulta plausible y aconsejable limitar, en la medida que sea posible, la utilización de estos medios; ello en razón de que este supuesto permite la publicación de un dato personal – notas de alumnos – en un sitio electrónico, el que abre el acceso a cualquier persona y en cualquier lugar del mundo, haciendo que tales datos ya publicados permanezcan eternamente en internet, lo que lleva a concluir que, para proteger precisamente a sus titulares, debiese actuarse más restrictivamente a este respecto.

Así las cosas, es que en este sentido la Ley 30/1992 permite limitar la publicidad cuando se vea afectada la intimidad de las personas[35] y consecuentemente con ello y en miras al equilibrio de intereses entre el derecho

[34] TRONCOSO, Op. Cit. Pág. 120.

[35] Este es el criterio que sigue ampliamente España al publicar en sitios web con claves para los interesados los resultados parciales de oposiciones o cuando se publican en el Boletín Oficial sólo las personas que han aprobado unas oposiciones, no las que han suspendido. A modo de ejemplo: una persona que trabaja en un estudio jurídico o en una consultora y que pretenda ingresar a la Administración, puede sentirse gravemente perjudicado/a si otra persona, por ejemplo su jefe, que no tiene ningún interés en el procedimiento administrativo ni en su transparencia, conoce a través de internet su participación en el mismo.

a la protección de datos – derecho fundamental bajo la legislación española – y el principio de transparencia administrativa, el criterio apunta a limitar el acceso en los sitios web sólo a aquellas personas que tuvieran un interés legítimo en el procedimiento administrativo, mientras que se impediría el acceso a personas que no tuvieran ningún interés en el mismo, respetándose de esta manera derecho a la protección de datos como los bienes jurídicos que respaldan la publicidad.[36]

Básicamente lo que refiere este punto es que el objetivo del sistema es permitir la comparación de los resultados y facilitar las posibles quejas al respecto. Y en cualquier caso, los resultados escolares deberían publicarse únicamente cuando sea necesario, y sólo después de informar a los alumnos y sus representantes del objetivo de la publicación y su derecho de oposición. En caso de riesgos – inherentes a este modo de comunicación – se exige que el acceso a los datos sea posible con salvaguardias especiales, utilizando sitios webs seguros o contraseñas personales asignadas a los representantes, o a cuando sean maduros, a los niños.[37]

[36] TRONCOSO, Op. Cit. Pág. 146.

[37] GRUPO DE TRABAJO 29. 2008. Documento de trabajo 1/08 sobre protección de datos personales de los niños (Directrices Generales y el caso especial de los colegios). Pág. 14 [En línea] < http://www.avpd.euskadi.eus/s04-redaneto/es/contenidos/informacion/redaneto/es_redaneto/adjuntos/informe_europeo_proteccion_datos_colegios.pdf > [Consulta: 28 de agosto de 2016]

4.a) El tratamiento de datos personales en los órganos públicos que integran el sistema educacional

En primer término señalar que de acuerdo a nuestra legislación es posible la comunicación de datos entre órganos de la Administración Pública sin consentimiento del interesado, en aquellos casos en que se ejerce competencias semejantes o cuando versen sobre las mismas materias. Ello pues en este caso se trata de una comunicación de datos personales entre órganos de la Administración del Estado que respeta el principio de finalidad, que se desarrolla para el ejercicio de las mismas competencias administrativas y sobre las mismas materias, autorizándose la comunicación y no exigiendo otra habilitación legal más específica, básicamente porque – como se señaló - este tratamiento respeta el principio de finalidad.[38] Por tanto, en nuestra realidad nacional será posible la comunicación de datos desde una escuela básica pública a la Superintendencia de Educación, al Ministerio de Educación o viceversa, en atención a que el tratamiento de la información al interior de una misma persona jurídica que tiene atribuida competencia administrativa educativa y que se desarrolla respetando la finalidad del registro será siempre

[38] En este punto valga destacar la distinción entre cesión de datos y comunicación de los mismos, puesto que el primero de ellos refiere a – en el caso de la tesis - cuando un establecimiento público de educación entrega toda la base de datos que posea respecto de sus alumnos; mientras que la comunicación estará referida sólo a datos específicos.

permitida, independientemente de si la declaración del fichero es centralizada o descentralizada.[39]

La Ley N° 19.628 dispone que los órganos públicos podrán realizar operaciones de tratamiento de datos dentro de la órbita de su competencia y de acuerdo a las condiciones que establece la ley, resaltando como única particularidad que se podrán realizar estas operaciones sin necesidad del previo consentimiento del afectado o del titular de los datos personales.[40] Lo anterior resulta relevante de destacar, puesto que sobre esa base se legitiman entidades como el Ministerio de Educación, Superintendencia de Educación, la Junta Nacional de Auxilio Escolar y Becas, y las corporaciones de educación municipal, entre otras – en el ámbito en análisis -, y se les permite realizar operaciones de tratamiento respecto de datos personales generados en o con ocasión de las finalidades educativas.[41]

[39] Para el profesor Antonio Troncoso Reigada, dentro de una misma Administración no habría cesiones de información, sino accesos a datos personales que deben respetar el principio de finalidad. Señala que el nivel de declaración de registros, efectuado en virtud de la atribución de determinadas responsabilidades y que puede ser más centralizado o descentralizado no puede suponer la existencia de una cesión, en atención a que se encontrarían en el marco de una misma persona jurídica.

[40] "*El tratamiento de datos personales por parte de organismo público sólo podrá efectuarse respecto de las materias de su competencia y con sujeción a la reglas precedentes. En esas condiciones, no necesitará el consentimiento del titular."* Artículo 20, Título IV "*Del tratamiento de datos por los organismos públicos*", Ley N° 19.628.

[41] DONOSO, Op. Cit. Pág. 15.

Sin embargo, cabe resaltar la importancia de distinguir entre la competencia para requerir datos y la competencia para el tratamiento de los mismos, pues en el caso que nos convoca en esta tesis podría darse la situación que en virtud de colaboraciones puedan cederse y/o comunicarse datos entre órganos públicos que no posean la misma competencia administrativa. En este contexto podría considerarse la colaboración entre una escuela pública y Servicio de Registro Civil e Identificación, donde se hace necesario que el colegio consulte del órgano público encargado de dejar constancia de los hechos o actos relativos al estado civil de las personas naturales y otros que las leyes le encomienden, antecedentes relativos a – por ejemplo - discapacidades de algún (os) menores de edad. En estos casos no se trata de órganos que posean las mismas competencias, pues el colegio público tendrá competencia educativa y competencia para requerir el dato, mientras que el Servicio de Registro Civil e Identificación sólo tendrá competencia para tratar los datos, en este caso de niñas, niños y adolescentes. En consecuencia, y entendiendo la diferencia en su actuar administrativo, igualmente procederían tales cesiones y/o comunicaciones, en virtud del cumplimiento del principio de cooperación y colaboración, amén del cumplimiento de la Ley Nº 19.628.

En este punto reiterar que, si bien la norma exime del deber de obtener el consentimiento previo del afectado, en ningún momento autoriza a no informar a los interesados sobre el tratamiento de datos que se está realizando,

imponiéndoseles además a los órganos públicos involucrados los deberes de respeto a los principios de calidad, finalidad, seguridad, responsabilidad, etc.

Por tanto, en todos los casos, a los alumnos, sus padres o quien tenga su representación, deben ser comunicados escrupulosamente y con carácter previo a la recogida de sus datos (ya sea a través de los formularios de solicitud de vacante y matrícula, de la ficha que el profesorado utiliza para el control de sus alumnos y alumnas o a través de cualquier otro canal de recogida) de la finalidad para la que éstos se recogen, de los destinatarios de la información que faciliten, del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas, de las consecuencias de la obtención de los datos o de la negativa a suministrarlos, de la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición, así como de la identidad y dirección del responsable del tratamiento.[42]

Cabe destacar además que en caso de ser la comunicación dirigida a menores de edad, debe expresarse en un lenguaje que sea fácilmente comprensible por ellos; lo anterior de conformidad a lo dispuesto en el artículo 13 del Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos

[42] CONSERJERÍA DE EDUCACIÓN. 2011. Guía de Protección de Datos de Carácter Personal para los Centros de Enseñanza. (Ley Orgánica 15/1999, de 13 de diciembre, y Real Decreto 1720/2007, de 21 de diciembre, Junta de Andalucía, 1° Edición, España. Pág. 74. [En línea] < http://www.juntadeandalucia.es/educacion/portalseneca/c/document_library/get_file?uuid=a3b83621-b564-48c3-ad8d-519dd7ced581&groupId=10128 > [Consulta: 14 de julio de 2016]

española,[43] la que si bien es de aplicación local del país ibérico, podría ser considerada exigible en nuestro país.

4.b) La información y el consentimiento para la formación docente

Cuando nos referimos a datos personales de niñas, niños y adolescentes en poder de establecimientos públicos de educación, entendemos que no se trata de cualquier antecedente administrativo, pues éstos contienen datos de relevancia que eventualmente pudieran afectar la vida privada del menor y que sólo pueden ser entregados en la medida que exista autorización del titular del mismo, o bien una orden legal que así lo disponga; ello, sin perjuicio de lo dicho en el numeral 4.a) sobre el tratamiento de datos personales en órganos públicos que integran el sistema educativo. En tal sentido, si tales datos están en manos de establecimientos educacionales nos encontraremos con un escenario en que la cantidad de datos personales y/o sensibles que requieren tratamientos suelen ser abundantes y en ocasiones complejos de tratar.

En ese plano y específicamente referido a alumnos, el establecimiento dispondrá, por ejemplo, de datos relativos a sus asistencia; antecedentes sobre la puntualidad de éstos, las notas obtenidas, los libros solicitados en la

[43] Ibid, Pág. 75.

biblioteca, las anotaciones conductuales que de alguna manera denotarán los hábitos de un alumno, como así también antecedentes que dicen relación con enfermedades que pueda padecer, inclusive de los medicamentos que se le administren. A lo anterior debe adicionarse aquellos datos que son objeto de tratamiento por parte de otras entidades, de terceros ajenos a la institución educadora, pero que son tratados por ésta, como por ejemplo, las licencias médicas del estudiante o sus informes sociales, antecedentes que abultan de manera insospechada y casi ilimitada la cantidad de datos personales que pueda tratar un jardín de infantes o un colegio y que en algunas ocasiones tienen un alto grado de sensibilidad.[44]

En este punto valga vincular nuestra legislación con la Convención de la Organización de las Naciones Unidas sobre los Derechos del Niño,[45] que considera a los menores como sujetos de derechos humanos y civiles, con algunas prevenciones especiales referidas al ejercicio de sus derechos, en función de su edad y madurez y de la salvaguarda de los derechos de sus padres y cuidadores. El derecho del niño a ser oído y a que su opinión sea debidamente tomada en cuenta se encuentra consagrado en el artículo 12 de la citada Convención como uno de los pilares fundamentales donde se asienta

[44] DONOSO, Op. Cit. Pág. 62.

[45] Convención aprobada en la Asamblea General de ese organismo internacional, el 20 de noviembre de 1989. En Chile es derecho vigente desde la publicación del Decreto Supremo Nº 830, de 27 de septiembre de 1990.

esta nueva concepción del niño como sujeto de derechos, debiendo los Estados de garantizar la libertad de pensamiento y expresión de los menores, regulando expresamente el derecho de los niños a ser oídos en todas las decisiones que puedan afectar su vida futura, fijando así pautas interpretativas que sirvan de guía tanto al juez como al legislador.

A nivel internacional la interpretación tradicional, tanto en la teoría general de los derechos como en el ámbito de la protección de datos personales, es que a partir de los 14 años una persona dispone de condiciones de madurez para otorgar consentimiento y para ejercer los derechos que éste supone; consecuentemente antes de esa edad, por regla general, será el representante legal quien deberá actuar y consentir a su nombre en aquellos casos en que el afectado se encuentre en situación de incapacidad o de minoría de edad que le imposibilite el ejercicio personal de sus derechos.[46] A este respecto la Agencia Española de Protección de Datos - AEPD – ha señalado que las personas mayores de catorce años reúnen las condiciones suficientes de madurez para prestar su consentimiento al tratamiento de los datos, toda vez que el ordenamiento jurídico, en diversos casos, reconoce a los y las mayores de 14 años la suficiente capacidad de discernimiento y madurez para adoptar por sí

[46] En Chile, de acuerdo a lo dispuesto en el Código Civil una persona de 14 años, de acuerdo a las reglas de capacidad, se presenta como un incapaz relativo, al ser considerado un menor adulto ante el ordenamiento jurídico. (Mujer: 12 a 18 años; Varón: 14 a 18 años)

solos/as determinados actos de la vida civil (adquisición de la nacionalidad española por ejercicio del derecho de opción o por residencia, capacidad para testar, etc.), y respecto de los y las restantes menores de edad, la AEPD entiende que no puede ofrecerse una solución claramente favorable a la posibilidad de que por los/las mismos/as pueda prestarse el consentimiento al tratamiento, por lo que la referencia deberá buscarse en el artículo 162, número 1º del Código Civil, tomando en cuenta, fundamentalmente, sus condiciones de madurez.[47] En este sentido, cabe precisar que en España no basta con ser menor de edad para que los derechos puedan ser ejercidos por el representante legal, sino, como ya indicamos, será menester que se trate de una minoría de edad que imposibilite el ejercicio personal de los mismos.[48]

En nuestro país, la Ley Nº 19.628 nada ha señalado al respecto ni tampoco ha fijado limitaciones para el ejercicio del derecho por parte de los menores, pues sólo refiere que el ejercicio del derecho de acceso, de modificación, cancelación o bloqueo le corresponde al titular de los datos, debiendo entenderse, para estos efectos, que serán los padres y/o apoderados quienes ejerzan este derecho a nombre del menor en caso de ser requeridos.

[47] CONSERJERÍA DE EDUCACIÓN, Op. Cit. Pág. 176.

[48] AGENCIA DE PROTECCIÓN DE DATOS de la Comunidad de Madrid, Op. Cit. Pág. 62.

La profesora Lorena Donoso Abarca, ha sostenido que en aquellos casos en que se requiere información relativa a la hoja de vida de un menor en el sector educación que: "*los datos personales de los menores que son tratados en el sistema educacional no pueden considerarse como provenientes de fuentes de acceso al público para proceder a su revelación* (artículo 7° de la Ley Nº 19.628)[49] *y merecen protección pese a las falencias de nuestra legislación en la materia, especialmente teniendo en consideración que uno de los principios de nuestra legislación es el del interés superior del niño*" . En esta misma línea de argumentación, la Convención de Derechos del Niño, en su artículo 16.1, establece que *"Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación"*, razón por la que sus antecedentes deben ser tratados con estricto apego a la norma y con especial atención en virtud de sus particulares características.

[49] Artículo 7, Ley Nº 19.628: *"Las personas que trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligados a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con el banco de datos, obligación que no cesa por haber terminado sus actividades en ese campo."*

CAPÍTULO SEGUNDO

OBLIGACIONES DE LOS ESTABLECIMIENTOS EDUCATIVOS PÚBLICOS Y DERECHOS DE LOS TITULARES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

1) Contexto

Sabido es que nuestra legislación en el ámbito de protección de datos personales es deficiente. La Ley Nº 19.628 es un cuerpo normativo que regula en términos generales el amparo que debe otorgársele a ciertos antecedentes que revisten el carácter de personales y sensibles, que por ser bienes jurídicos relevantes necesitan protección. Se sostiene que – y aun en discusión parlamentaria - su deficiencia radica también en la inexistencia de una autoridad de control independiente que vele por el cumplimiento de la ley por parte de los organismos privados, que tenga las facultades de imponer sanciones por el incumplimiento y que tenga un rol de promoción de la protección de datos personales.

No encontramos entonces una normativa especial aplicable a un área específica, como por ejemplo en el ámbito de la educación; por tanto, en caso de enfrentarse un establecimiento educativo a la necesidad de proteger datos personales sólo dispondrá de la Ley Nº 19.628, del Reglamento del Registro de Bancos de Datos Personales a cargo de Organismos Públicos, y Recomendaciones emanadas del Consejo para la Transparencia para hacer frente a esta labor de amparo.

Consecuencia de lo anterior es que tampoco existe respecto de los individuos afectados (alumnos, personal docente, administrativos) claridad en relación a dónde recurrir en caso de una vulneración al derecho de protección de datos personales; discusión que actualmente se encuentra en la palestra, pero que aún no ha encontrado cabida legal – real - en nuestro ordenamiento jurídico.

En virtud de lo señalado, es que se hace necesario observar la legislación comparada, para de esta manera establecer y determinar cuáles son las obligaciones que pesan sobre los establecimientos de educación en materia de protección de datos.

El presente capítulo toma entonces de la legislación comparada, específicamente española y mexicana, las principales obligaciones y también

los derechos que deben cumplir los establecimientos educativos para hacer frente a la protección de datos personales.

En primer lugar tomaremos el ejemplo de España, país que cuenta con una robusta legislación en la materia que nos ocupa. Estableció una institucionalidad a través de la Agencia Española de Protección de Datos – AEPD -, órgano encargado de velar precisamente por el amparo de este derecho, que en su caso ostenta rango constitucional y que se apoya en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal – LOPD –[50]

Cabe señalar que además de la referida Agencia, en España existen agencias de protección de datos de carácter autonómico en Cataluña y en el País Vasco,[51] las que se constituyen como autoridad de control para garantizar el derecho fundamental de protección de datos personales relativos a los ficheros de titularidad pública creados o gestionados por los entes que integran la Administración local y regional, las Universidades o las Corporaciones de Derecho Público.

[50] Última modificación: 05 de marzo de 2011.

[51] El 25 de septiembre de 2012, la Comunidad de Madrid anunció la supresión de la Agencia de Protección de Datos de la Comunidad de Madrid, lo que se materializó el 1 de enero de 2013. Sus funciones pasaron a ser asumidas íntegramente por la Agencia Española de Protección de Datos.

La Directiva 95/46/CE[52] como la LOPD entienden por fichero cualquier tratamiento de datos personales, sea o no automatizado, siempre que estén estructurados de forma que permitan un fácil acceso a la información relativa de una determinada persona. De hecho, mucha información personal dentro de la administración educativa se encuentra almacenada en ficheros manuales-estructurados, razón por la que el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal – RDLOPD-, [53] estableció las medidas de seguridad que éstos deben seguir.[54]

Atendido lo anterior y en primer lugar, para poder cumplir la legislación de protección de datos personales, es necesario conocer qué tratamientos de datos personales lleva a cabo un colegio, por lo que debe procederse a la identificación de los ficheros de datos personales que se manejan. Entre ellos

[52] DIRECTIVA 95/45/CE del Parlamento Europeo y del Consejo del 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Su objetivo es garantizar la protección de las libertades y de los derechos fundamentales de las personas físicas, y en particular, del derecho a la intimidad en lo que respecta al tratamiento de los datos personales. Esta Directiva sostiene los siguientes lineamientos: i. Reconoce que los sistemas de tratamiento de datos están al servicio del hombre y deben respetar las libertades y derechos fundamentales de las personas físicas, y en particular, la intimidad; ii. Reconoce las diferencias existentes en las legislaciones de los Estados miembros, respecto de los niveles de protección de los datos personales, lo que crea obstáculos en la circulación de los mismos; iii. Promueve la armonización de las legislaciones que protegen los datos personales buscando ofrecer un nivel máximo de garantía a los ciudadanos de la Unión Europea; iv. Los Estados miembros dispondrán la transferencia de datos personales a un país tercero únicamente cuando el país tercero garantice un nivel de protección adecuado. Recordar la entrada en vigencia el año 2018 del Reglamento Europeo de Protección de datos, que derogará a la Ley Orgánica 15/1999 y al Real Decreto 1720/2007.

[53] Última modificación: 08 de marzo de 2012.

[54] AGENCIA DE PROTECCIÓN DE DATOS de la Comunidad de Madrid, Op. Cit. Pág. 28.

sobresalen algunas funciones que requieren tratamiento: matrícula y admisión de alumnos que recoge datos identificativos, características personales, circunstancias sociales, datos económicos y sociales tanto de alumnos como de sus familiares, etc.; además de otros servicios complementarios como el servicio de comedor y el de transporte de alumnos que también implican la utilización de datos identificativos y económicos de éstos; el almacenamiento de claves de usuario de acceso a un espacio privado en Internet o en una intranet y el de cuentas de correo electrónico, lo que supone un tratamiento de la dirección TCP/IP,[55] que llama a ser consciente, a prevenir la declaración del fichero correspondiente y el cumplimiento de los principios y los derechos de protección de datos.[56]

Como punto de partida en esta materia debe tenerse presente que no es posible el tratamiento de datos, ya sea en registros automatizados, manuales o parcialmente automatizados, sin cumplir los procedimientos formales y sustantivos. Es por ello – y tomando en consideración la legislación española - que los establecimientos de educación deben responsabilizarse de cumplir ciertas obligaciones al respecto; las que en términos generales son:

[55] La dirección TCP/IP es el protocolo básico de transmisión de datos en Internet, que como regla general, supone un dato de carácter personal ya que normalmente existe un fichero histórico con la dirección IP (fija o dinámica) asignada a cada puesto, el número de identificación del suscriptor, la fecha, la hora y la duración de la asignación de dirección. Obviamente, resulta más sencillo identificar a los usuarios de Internet que utilizan direcciones estáticas.

[56] AGENCIA DE PROTECCIÓN DE DATOS de la Comunidad de Madrid, Op. Cit. Pág. 30.

i. Recoger y tratar adecuadamente los datos: Los formularios, o cualquier otro elemento o procedimiento utilizado para recoger datos personales, deberán adecuarse al principio de calidad y al principio de finalidad.

ii. Facilitar el ejercicio de los derechos que otorga el sistema de protección de datos personales: Esto referido a hacer más asequible a quienes lo soliciten y especialmente a los alumnos, padres y/o apoderados o representantes legales, el ejercicio de sus derechos de acceso, rectificación, oposición y cancelación sobre sus propios datos.

iii. Garantizar la seguridad en el tratamiento de datos personales: Ello, a través de la creación e implementación de medidas de carácter técnicas y organizativas que incluyan la elaboración de documentos de seguridad, garantizando además estos aspectos cuando el tratamiento de datos personales sea realizado por un tercero a cuenta del establecimiento educativo, mediante la incorporación de cláusulas específicas en los contratos, amén de la supervisión de su cumplimiento.

iv. Realización de auditorías de los ficheros: Obligación que tendrá lugar en aquellos casos en que los ficheros tengan nivel de seguridad medio o alto.[57]

[57] AGENCIA DE PROTECCIÓN DE DATOS de la Comunidad de Madrid, Op. Cit. Pág. 111 y ss.

A este respecto valga mencionar la dictación del nuevo Reglamento Europeo de Protección de Datos 2016/679,[58] texto que unifica en toda la Unión Europea la regulación de la protección de los datos personales, avanzando así en la defensa, garantías y libertades de los datos personales de los ciudadanos europeos, alcanzando una homogeneidad en su protección, otorgándoles un mayor control sobre sus propios datos y reforzando la seguridad que conceden tanto empresas como organismos públicos. Dicho Reglamento entrará en vigor a los 20 días tras su publicación en el Diario Oficial de la Unión Europea si bien sus disposiciones resultarán de aplicación directa a todos los Estados Miembros pasados dos años desde su publicación, esto es, el próximo 25 de mayo de 2018, y por tanto, formarán parte de los ordenamientos jurídicos europeos sin necesidad de que sea traspuesto por una norma nacional.[59] Es por ello que, hasta entonces tanto la Directiva 95/46 como las normas nacionales españolas que la trasponen, siguen siendo plenamente válidas y aplicables**.**

En virtud de lo anterior, el período de dos años hasta la aplicación del Reglamento tiene como objetivo permitir que los Estados de la Unión Europea como las organizaciones que tratan datos vayan preparándose y adoptándose para el momento en que el Reglamento sea aplicable. Ello, ya sea adoptando o

[58] Aprobado por el Parlamento Europeo el 14 de abril de 2016, que sustituye y renueva la anterior Directiva 95/46/CE.

[59] NUNSYS. Consultorías y Seguridad. Novedades del Nuevo Reglamento Europeo de Protección de Datos, España. Pág. 2. [En línea] <http://nunsys.com/Descargar/adaptacion-reglamento-proteccion-datos.pdf> [Consulta: 12 de agosto de 2016]

iniciando la elaboración de determinadas normas que sean necesarias para permitir o facilitar la aplicación del Reglamento, las que no pueden ser contrarias a las disposiciones de la vigente Directiva ni tampoco ir más allá de los poderes de actuación normativa que el propio Reglamento prevé de forma explícita o implícita.

En consecuencia, en España – nuestro país europeo de referencia para estos efectos - los responsables de ficheros de datos, entre ellos establecimientos educacionales, siguen teniendo las obligaciones que indica la Directiva 95/46/CE y la Ley Orgánica 15/1999, entre las que se encuentran las siguientes:

2) Obligaciones de establecimientos educativos en materia de protección de datos

2.a) Creación y actualización de ficheros utilizados para el almacenamiento de datos personales de alumnos

La primera obligación que deben cumplir los responsables públicos del tratamiento de datos personales es crear sus ficheros o registros y notificarlos a la Agencia de Protección de Datos, los que conforme a la Ley Orgánica Nº 15/1999, sólo pueden ser creados, modificados o suprimidos por medio de una

disposición de carácter general publicada en el “Boletín Oficial del Estado” o en el Diario Oficial, siendo obligatoria su inscripción en el Registro General de Protección de Datos – RGPD -.

Para efectos de la declaración de ficheros o registros de datos personales los establecimientos educativos deben: a) Identificar e inventariar los ficheros y tratamientos en los que se almacenen datos personales que deben ser objetos de declaración. Por ejemplo: Qué datos personales se tienen que recoger y para qué finalidad; cómo se recogerán (formularios en papel, electrónicamente); qué ficheros hay que crear y, si procede, qué ficheros hace falta modificar o suprimir; quién los tratará; cómo circularán dentro de la entidad; a quién se cederán o qué transferencias internacionales se harán; cómo se conservarán y, si procede, cómo y cuándo se destruirán; b) Aprobar y publicar la Disposición de carácter general de creación, modificación o cancelación de los ficheros y tratamientos; c) Notificar, telemáticamente o mediante el envío de impresos oficiales, los ficheros o tratamientos al Registro de Ficheros de Datos Personales de la AEPD.[60]

Por su parte, para la realización del proceso de Notificación de ficheros de titularidad pública es requisito previo que se haya publicado una disposición que contenga la descripción completa del fichero que incluya los siguientes ítems:

[60] AGENCIA DE PROTECCIÓN DE DATOS de la Comunidad de Madrid, Op. Cit. Pág. 113.

su nombre, su finalidad y usos previstos, los colectivos de los que se pretende recabar datos de carácter personal así como los procedimientos empleados para su obtención, la estructura de los datos al igual que el sistema de tratamiento empleado y las posibles cesiones o transferencias internacionales de datos que sufrirán estos.

Los ficheros se inscriben una vez verificado el cumplimiento de los requisitos establecidos en la LOPD y el RLOPD y habiendo transcurrido un mes desde la presentación de la solicitud de inscripción sin que se haya resuelto, el fichero se entenderá inscrito a todos los efectos.[61]

Importante señalar que la inscripción de los ficheros debe encontrarse actualizada en todo momento, por lo que cualquier modificación que afecte al contenido de la inscripción debe ser notificada a la AEPD para proceder a su rectificación. Cuando el responsable de un fichero decida su supresión, debe notificarla con el objetivo de que procediera a la cancelación de la respectiva inscripción.

[61] APDCAT (Agencia de Protección de Datos de Cataluña). 2014. Guía básica de protección de datos para los centros educativos. Generalitat de Catalunya Autoritat Catalana de Protecció de Dades, España. Pág. 54. [En línea] < http://www.apd.cat/media/2891.pdf > [Consulta: 21 de julio de 2016]

Para los efectos descritos y en el caso español es menester distinguir:

a) Ficheros de datos de carácter personal de titularidad pública: Deben ser notificados a la AEPD por el órgano competente de la administración responsable para su inscripción en el RGPD en el plazo de treinta días contados desde la publicación de su norma o acuerdo de creación en el Diario Oficial correspondiente.
b) Ficheros de datos de carácter personal de titularidad privada: Deben ser notificados a la AEPD por la persona o entidad privada que pretendía crearlos, con carácter previo a su creación.

Las inscripciones se realizan sólo si las notificaciones se ajustan a los requisitos exigibles, siendo esta inscripción totalmente gratuita.[62]

Una vez inscrito correctamente el fichero en el RGPD, se notifica la resolución de inscripción del Director de la Agencia, comunicándole el código de inscripción asignado y la dirección que se ha hecho constar en el apartado correspondiente de la hoja de solicitud.[63] En caso que los interesados así lo

[62] No se encuentran dentro del ámbito de aplicación de la LOPD, y por tanto no deben notificarse, los tratamientos referidos a personas jurídicas, ni a los ficheros que se limiten únicamente a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales. Tampoco deberán notificarse los ficheros con datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros.

[63] A través del Servicio de Notificaciones Electrónicas (https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/Notificaciones_tele

manifiesten expresamente en el formulario de notificación, podrán recibir por medios telemáticos la notificación de la resolución de inscripción, la comunicación de la necesidad de subsanar su requerimiento, o cualquier otro escrito relacionado con la solicitud de inscripción de ficheros en el RGPD, para lo que deberán disponer de una dirección electrónica a efectos de notificaciones del Servicio de Notificaciones Telemáticas Seguras.[64]

Posterior a tales diligencias, se da comienzo al procedimiento rellenando el formulario respectivo, en el cual se realizan una serie de preguntas de control sobre el tipo de solicitud, modelo de declaración y modo de presentación, con el objetivo de obtener la mayor cantidad de antecedentes que permitan una correcta y adecuada inscripción del respectivo fichero.[65]

Items considerados en el citado formulario:

Item Nº 1: Responsable del Fichero.

/index-ides-idphp.php), se pone a disposición de cualquier persona física o jurídica que lo solicite la posibilidad de recibir de forma alternativa por vía telemática las notificaciones que actualmente reciben en papel. La suscripción a este servicio es voluntaria y tiene carácter gratuito.

[64] SISNOT es una aplicación desarrollada por el Ministerio de Hacienda y Administraciones Públicas, que incluye todos los módulos de integración con el Servicio de Notificaciones telemáticas seguras y realiza las funciones necesarias para descargar a las aplicaciones de la gestión de la conexión con el servicio, siendo una herramienta que proporciona un interfaz de Web Service a las aplicaciones de gestión de procedimientos. Está desarrollado en software no licenciable y puede utilizar como base de datos: Oracle, SQL Server o Postgres. Además SISNOT se proporciona de forma gratuita.

[65] LÁZARO DE RAFAEL, B., 2009. Registro de un fichero de datos personales con el formulario NOTA. España. [En línea] <http://www.adictosaltrabajo.com/tutoriales/inscripcion-fichero-datos/> [Consulta: 25 de julio de 2016]

Item Nº 2: Derechos de oposición, acceso, rectificación y cancelación.

Item Nº 4: Encargado del tratamiento.[66]

Item Nº 5: Identificación y Finalidad del fichero.

Item Nº 6: Origen y procedencia de los datos.

Item Nº 7: Tipos de datos, estructura y organización del fichero.[67]

Item Nº 8: Medidas de Seguridad.

Item Nº 9: Cesión o comunicación de datos.

Item Nº 10: Transferencias Internacionales.

Una vez rellenado todos los puntos requeridos, se exige completar la hoja de solicitud que recoge todos los datos que se han introducido en todos los puntos anteriores, adicionando la información personal de la persona física – natural - que presenta la solicitud en la AEPD y una dirección de contacto para recibir las notificaciones relativas al fichero por parte de la Agencia.[68]

---

[66] En este ítem es necesario aclarar que la solicitud de inscripción de un nuevo fichero no permite completar en el formulario el ítem N° 3 correspondiente al *"encargado del tratamiento",* debiéndose en este caso indicar que la prestación de servicio implica que el fichero se encuentre ubicado en los locales del encargado del tratamiento.

[67] Puede suceder que el tratamiento de datos contenga de aquellos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, casos en los que con motivo del cumplimiento de deberes públicos, deberán implantarse medidas de seguridad de nivel básico" (Art.81.6 Reglamento de desarrollo de la LOPD)
En este mismo sentido, es muy común que los formularios de recogida de datos tengan apartados del tipo intereses, aficiones, etc., los que podría ser utilizados para elaborar un perfil de la persona, motivo por el que la LOPD obliga a mantenerlos bajo un nivel de seguridad medio, a menos que haya otros datos que obligue al nivel máximo.

[68] LÁZARO DE RAFAEL, Op. Cit.

Para efectuar Modificación de la inscripción de un fichero previamente inscrito en el RGPD, la obligación consiste en completar el formulario electrónico, la hoja de solicitud, el apartado de Modificación de la inscripción del fichero, indicando el código de inscripción asignado por la Agencia y señalando aquellos apartados que se modifican respecto a la notificación anterior.[69] Para el caso de la supresión de fichero, se indicará el motivo de la supresión en el texto correspondiente y el destino de la información en el siguiente campo. En el caso de proceder a destruir el fichero, se debe indicar las previsiones adoptadas para ello.[70]

Una vez que se cumplen las dos etapas anteriores y los formularios se encuentran rellenados, el interlocutor con la Agencia Española de Protección de Datos lleva a cabo los trámites necesarios para que sea aprobado el proyecto de disposición que regulará la creación, modificación o supresión de los ficheros.[71]

[69] Según las instrucciones que acompañan al formulario.

[70] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Inscripción de Ficheros, Preguntas más frecuentes. [En línea] <https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/preguntas_frecuentes/cuestiones_generales/index-ides-idphp.php > [Consulta: 10 de agosto de 2016]

[71] En el ámbito educativo, los antecedentes se remiten a la Subdirección General de Régimen Jurídico de la Secretaría General Técnica de la Conserjería de Educación, que tendrá la misión de revisar la documentación entregada.

Finalmente, en aquellos casos de inscripción en el Registro General de Protección de Datos de los ficheros de titularidad pública, una vez recibida la notificación de creación, modificación o supresión de ficheros de titularidad pública, si contuviera la información preceptiva y se cumplieran los restantes requisitos legales, el Director de la AEPD dicta resolución acordando el alta, modificación o supresión de los ficheros. Con el alta se asignará un código de inscripción, que se comunicará al responsable con la resolución y que será necesario para posteriores notificaciones de modificación o supresión.[72] Si la notificación no contuviese la información preceptiva o se advirtiesen defectos formales, el RGPD requerirá que se complete o se subsane; para el caso que la subsanación precisare la modificación de la disposición de carácter general el plazo es de tres meses.[73] En esta última situación, sin perjuicio del plazo de tres meses para la subsanación de defectos, la duración máxima del procedimiento es de un mes, entendiéndose inscrito, modificado o suprimido el fichero si no se hubiese dictado y notificado en dicho plazo la correspondiente resolución.[74]

Importante es mencionar que el nuevo Reglamento elimina la obligación de inscribir los ficheros; sin embargo dispone que deberá aplicarse la protección de datos por diseño y por defecto, además de evaluaciones de impacto ante

[72] Artículo 132 del Reglamento de Ley Orgánica de Protección de Datos, España.

[73] Artículo 131.2 del Reglamento de Ley Orgánica de Protección de Datos, España.

[74] Artículo 134 del Reglamento de Ley Orgánica de Protección de Datos, España.

determinados tratamientos de datos.[75] Se trata de uno de los requisitos más interesantes en el nuevo documento europeo, pues exige que el responsable del tratamiento de datos personales, lleve a cabo, antes de ese tratamiento, una evaluación de impacto relativa a la misma; evaluación que debe valorar la particularidad gravedad y probabilidad al alto riesgo, considerando la naturaleza, ámbito, contexto y fines del tratamiento, como también los orígenes del riesgo.[76]

Lo anterior significa que, del estrecho vínculo con el principio de responsabilidad, se suprime la exigencia de notificar a la autoridad nacional correspondiente los ficheros de datos personales, pero se insiste en la necesidad de que todo aquel que trate datos de carácter personal, aplique, por defecto y desde que empiece a idear el sistema de tratamiento, las medidas técnicas y organizativas, apropiadas en función del riesgo que implique tal tratamiento que sean necesarios para asegurar que en todo momento se cumple con la normativa sobre protección de datos.[77] Entre las medidas a considerar, se encuentra la reducción al máximo el tratamiento de datos

[75] BENITO, R., 2016. Menores, DPO y nuevos principios en la Protección de Datos. Law&Trends. Best Lawyer, more Justice. España [En Línea] <http://www.lawandtrends.com/noticias/tic/menores-dpo-y-nuevos-principios-en-la-proteccion.html> [Consulta: 12 de agosto de 2016]

[76] BROCCA, M., 2016. El nuevo Reglamento de Protección de Datos. España. [En Línea] <https://marinabrocca.com/proteccion-de-datos/nuevo-reglamento-proteccion-datos/> [Consulta: 17 de enero de 2017]

[77] BENITO, Op. Cit.

personales; seudonimizar lo antes posible los datos personales; dar transparencia a las funciones y el tratamiento de datos personales, además de crear y mejorar los elementos de seguridad; ello con el objetivo de establecer la prevención por parte de las organizaciones que tratan datos, la “responsabilidad activa”, esto es, que se adopten las medidas que aseguren razonablemente que están en condiciones de cumplir con los principios, derechos y garantías que el Reglamento establece, pues actuar sólo en aquellos casos en que se haya producido una infracción es insuficiente como estrategia, puesto que una vulneración a la norma puede ocasionar daños a los interesados que pueden ser difíciles de compensar o reparar.

Valga señalar en este ítem la necesidad de información a las autoridades cuando la evaluación de impacto indique riesgo elevado, casos en los que – de acuerdo al nuevo Reglamento - debe consultarse a la autoridad de control cuando la iniciación de actividades de tratamiento arrojen una evaluación de impacto que muestra que, en ausencia de garantía, medidas de seguridad y mecanismos destinados a mitigar riesgos, el tratamiento entrañaría un alto riesgo para los derechos y libertades de las personas – naturales -, y el responsable del tratamiento considera que el riesgo no puede mitigarse por medios razonables en cuanto a tecnología disponible y costes de aplicación.[78]

[78] BROCCA, Op. Cit.

En nuestro ordenamiento jurídico, el artículo 22 de la Ley N° 19.628 es el único precepto que refiere a los registros que deben llevar los órganos públicos, el que será administrado por el Servicio de Registro Civil e Identificación. Señala la norma que será un Reglamento el que definirá el contenido de tales registros, tarea consignada en el Decreto N° 779 del Ministerio de Justicia[79] que establece que la inscripción en el Registro de Banco de Datos Personales debe contener, al menos, las siguientes menciones: 1) Nombre del banco de datos personales; 2) El organismo público responsable del banco de datos personales respectivo; 3) El RUT correspondiente al organismo público; 4) El fundamento jurídico de su existencia; 5) La finalidad del banco de datos; 6) El o los tipos de datos almacenados en dicho banco; y 7) Una descripción del universo de personas que comprende.

Revisado el sitio web del Servicio de Registro Civil e Identificación, el Ministerio de Educación – MINEDUC - dispone un total de 26 registros,[80] entre los cuales se incluyen, entre otros: Alumnos con Discapacidad Sensorial (visual, auditiva) SIMCE 4º básico ; Formulario de Acreditación Socioeconómicos; Postulantes programa Becas Chile; Nómina de alumnos prioritarios; Registro de Estudiantes del Programa de Integración Escolar (PIE); antecedentes que en

[79] DECRETO CON FUERZA DE LEY Nº 779, que aprueba Reglamento del registro de banco de datos personales a cargo de organismos públicos. Fecha de promulgación: 24 de agosto de 2000. Santiago, Chile. [En línea] < file:///C:/Users/jledezma/Downloads/DTO-779_11-NOV-2000.pdf> [Consulta: 02 de febrero de 2017]

[80] Fecha de revisión: 12 de mayo de 2017.

este caso, el MINEDUC catastra e ingresa para cumplimiento de la norma antes señalada.

2.b) Recogida y tratamiento de datos personales de alumnos

A este respecto debemos mencionar que el tratamiento de datos de carácter personal debe cumplir la normativa en materia de protección de datos en todas sus fases, desde la recogida de información hasta su archivo y mantenimiento.

Los datos que se recojan deben ser adecuados, pertinentes y no excesivos para la finalidad que se pretende, lo que implica que todos los formularios, cuestionarios o pantallas que recaben tales antecedentes deben ser diseñados velando porque la recolección cubra sólo aquellos datos que sean estrictamente necesarios.[81] Para el caso de obtención de consentimiento, éste deberá estar referido a un tratamiento o serie de tratamientos concretos, con clara delimitación de la finalidad para la cual se recaba, además de las restantes condiciones que concurran en el tratamiento o serie de tratamientos; los datos especialmente protegidos – sensibles -.

La legislación española, por ejemplo prevé en casos de antecedentes sensibles que, no obstante ser menester autorización para tratar datos, existe

[81] AGENCIA DE PROTECCIÓN DE DATOS de la Comunidad de Madrid, Op. Cit. Pág.138.

excepción respecto de aquellos casos en que tales datos resulten necesarios para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios; lo anterior, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

México exige la obligatoriedad de contar con el consentimiento del afectado en caso de tratar datos sensibles, indicando expresamente los casos en que no será necesario obtenerlo: Esté previsto en una ley; los datos figuren en fuentes de acceso público; en caso de someter los datos personales a procedimiento previo de disociación; cuando el tratamiento tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable; cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes; se dicte resolución de autoridad competente; y cuando – al igual que en España - sean indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, mientras el titular no esté en condiciones de otorgar el consentimiento, en los términos que establece la Ley General de Salud y demás disposiciones jurídicas aplicables y

que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente.[82]

En todos los casos siempre será obligatorio que el establecimiento educacional responsable del tratamiento de los datos informe a los interesados – padres y alumnos - al momento de la recogida de los mismos sobre los derechos que les asisten sobre sus propios datos personales; para ello, todos los formularios de recogida de datos – en formato papel o digital – debe incorporar información relativa a los derechos que les competen, con indicación de cómo hacerlos efectivos y el lugar para ello.

2.b.1) Deber de información en la recogida de datos personales

En nuestro país, la ley establece a este respecto que la persona que autoriza el tratamiento de sus datos personales debe ser debidamente informada sobre el propósito del almacenamiento de tales datos y su posible comunicación al público, lo que se traduce en que cada vez que un establecimiento escolar recabe datos, deberá informar su finalidad y la eventualidad de que los datos personales entregados puedan ser cedidos a terceros; de ello se desprende que la Ley N°19.628 no exige la indicación de los derechos que le asisten al

[82] Artículo 10, Ley Federal de Protección de Datos Personales en Posesión de los Particulares, México.

titular de los datos, como tampoco las consecuencias de no responder las preguntas planteadas, ni la exigencia de informar la identidad ni domicilio del responsable de ese tratamiento, lo que en definitiva constituye una falencia respecto precisamente de la protección de los datos.

En el caso español, el derecho a la información en la recogida de datos requiere se informe en cada formulario en forma claramente legible, de modo expreso, preciso e inequívoco lo siguiente: i. De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información; ii. Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas; iii. De las consecuencias de la obtención de datos o de la negativa de suministrarlos; iv. De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; y v. De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante. [83]

La Ley Orgánica 15/1999 dispone que cuando los datos de carácter personal no hayan sido recabados del interesado, éste debe ser informado expresa, precisa e inequívocamente por el responsable del fichero o su representante, dentro de los tres meses siguientes al registro de los datos, a excepción de ya

[83] Artículo 5, Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, España. Destacar que no será necesaria la información a que se refieren los numerales ii), iii) y iv) recién mencionados cuando del contenido de ellas se deduce claramente la naturaleza de los datos personales que se solicitan o las circunstancias en que se recolectan.

haber sido informados del contenido del tratamiento con anterioridad; [84] no será de aplicación lo antes dicho en aquellos casos en que expresamente una ley lo prevea, en caso de tratamiento de datos históricos, estadísticos o científicos, o bien cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados[85] en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias. Asimismo, tampoco regirá esta obtención de consentimiento cuando los datos procedan de fuentes accesibles al público, casos en que cada comunicación que se dirija al interesado deberá informarse de los datos, de la identidad del responsable y los derechos que le asisten;[86] ello con el objetivo que conozca de antemano para qué finalidad se van a tratar, y por quién, pudiendo además en cualquier momento ejercitar sus derechos de acceso, rectificación, cancelación u oposición.

Observando el caso mexicano, éste reproduce casi totalmente lo previsto en la ley española de protección de datos personales, indicando en su artículo 8 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares – LFPDPPP - que a través del “aviso de privacidad”, el responsable de un banco de datos deberá dar cumplimiento a la obligación de informar a los

[84] Artículo 5. 4. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. España.

[85] Según criterio de la Agencia de Protección de Datos Española.

[86] AGENCIA DE PROTECCIÓN DE DATOS de la Comunidad de Madrid, Op. Cit. Pág.140.

titulares de los mismos, la información que se recaba de ellos y los fines que éste contempla,[87] y que se entiende que el titular consiente tácitamente en el tratamiento de sus datos, cuando habiéndose dado noticia del aviso de privacidad, no manifieste oposición alguna.

El citado aviso de privacidad**,** deberá contener, al menos, la siguiente información: i. La identidad y domicilio del responsable que los recaba; ii. Las finalidades del tratamiento de datos; iii. Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos; iv. Los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuesto en esta Ley; v. En su caso, las transferencias de datos que se efectúen, y vi. El procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad, de conformidad con lo previsto en esta Ley. En caso de tratar datos personales de carácter sensibles, el aviso de privacidad deberá señalar expresamente que se trata de este tipo de datos.[88]

[87] Artículo 15, Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. España; artículo 16, Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

[88] Artículo 16, Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. España.; artículo 16 Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

2.b.2) Incumplimiento del deber de información

A este respecto la norma chilena nada prevé; recurrimos entonces a la ley española que establece que tal conducta se tipifica como falta leve, conforme al artículo 44.2.c) de la Ley Orgánica 15/1999, el que a su tenor señala: *"El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos sean recabados del propio interesado".* Por su parte, se típica como falta grave, según el artículo 44.3.c): *"El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos no hayan sido recabados del propio interesado"*.[89]

Del mismo modo, la ley mexicana, en su artículo 63, V dispone que el responsable se constituye en infractor a la Ley, si omite en el aviso de privacidad, alguno o todos los elementos a que se refiere el artículo 16, siendo sancionado su incumplimiento con multa de 100 a 160,000 días de salario mínimo vigente en el Distrito Federal.[90]

---

[89] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Canal del responsable de ficheros. Deber de Información. [En línea] <https://www.agpd.es/portalwebAGPD/canalresponsable/obligaciones/deber_informacion/index-ides-idphp.php> [Consulta: 18 de julio de 2016]

[90] Artículo 64, II Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

2.b.3) Consentimiento para el tratamiento de datos personales de menores

Sin perjuicio de lo señalado en el capítulo I, valga ahondar en lo que ha dispuesto para estos efectos la legislación española, la que resulta interesante en atención al razonamiento establecido en orden a otorgar a un menor la facultad de decidir respecto de la autorización para la entrega de datos personales. Se trata de una situación diversa a lo que ocurre en nuestro país, donde como ya hemos referido, el menor de 18 años es considerado un incapaz relativo y para efectos de la Ley de Protección de Datos deberán ser sus padres o quienes lo tengan a su cuidado quienes autoricen la entrega de antecedentes de aquél.

En España en la actualidad, sin perjuicio de la aplicación del nuevo Reglamento de Protección de Datos, el tratamiento de datos de menores de edad requiere de una vigilancia especial, ya que la Agencia Española de Protección de Datos exige mayor rigurosidad a su respecto; ello puesto que va dirigido a una persona más vulnerable. Entonces la interrogante que surge es, cuál es la frontera de edad respecto a quién se considera capacitado para proporcionar ese consentimiento, específicamente en el ámbito educativo. La respuesta, en el ordenamiento jurídico español no está sectorializada – al igual que en el caso chileno -, por lo que debe recurrirse al artículo 13.1 del

Reglamento LOPD, el que a su tenor señala: "*Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores"*. Por su parte, los requisitos exigidos por la LOPD para que el consentimiento sea válido son que debe de ser libre, inequívoco, específico e informado.

Cabe sostener además que el responsable del fichero es quien debe garantizar que el consentimiento obtenido es válido, debiendo asegurarse de que la persona que presta ese consentimiento es quien está capacitada para hacerlo; por ello la autoridad escolar debe adoptar las medidas necesarias para cerciorarse que el menor, quien consiente en el tratamiento de datos en el establecimiento educativo, tiene la suficiente capacidad; lo que usualmente hará requiriendo el DNI u otra forma de identificación a esa persona. [91]

En cuanto al nuevo Reglamento de Protección de Datos Europeo, precisamente en este ítem se produce una novedad que dice relación con oferta directa a niños de servicios de la sociedad de la información (comercio

[91] GONZÁLEZ, A., 2016. Consentimiento para el tratamiento de datos de menores de edad. Ayuda Ley Protección de Datos. España [En línea] <http://ayudaleyprotecciondatos.es/2016/07/28/tratamiento-de-datos-de-menores-de-edad/> [Consulta: 18 de enero de 2017]

electrónico, redes sociales), pues indica en su artículo 8 que el tratamiento de los datos personales de un niño se considerará lícito cuando éste tenga como mínimo 16 años; en caso de ser menor de esa edad, tal tratamiento se considerará lícito sólo si lo dio o autorizó el titular de la patria potestad o tutela del niño, y sólo en la medida que se dio o autorizó.[92] Sin perjuicio de lo anterior, los Estados Miembros podrán establecer por ley, una edad inferior a tales fines, siempre que ésta no sea inferior a 13 años.[93]

A este respecto indicar que en México, la Ley General de Educación[94] dispone en su artículo 70 letra e) que en cada municipio operará un consejo municipal de participación social en la educación que gestionará ante el municipio y ante la autoridad educativa local, entre otras, la tarea de coordinación de escuelas con autoridades que particularmente atiendan temas relacionados con la defensa de los derechos consagrados en la Ley de

[92] BROCCA, Op. Cit.

[93] MAYOR, R., 2016. Contenido y Novedades del Reglamento General de Protección de Datos de la UE (Reglamento UE 2016/679, de 27 de abril de 2016). Gabilex N° 16. España. [En línea] < http://www.castillalamancha.es/sites/default/files/documentos/pdf/20160709/revista_gabilex_no_6._autor_roberto_mayor_gomez.pdf > [Consulta: 17 de enero de 2017]

[94] LEY GENERAL DE EDUCACIÓN. México. Nueva Ley publicada en el Diario Oficial de la Federación el 13 de julio de 1993. Última modificación publicada DOF 01 de junio de 2016. Secretaría de Educación Pública. [En línea] < https://www.sep.gob.mx/work/models/sep1/Resource/558c2c24-0b12-4676-ad90-8ab78086b184/ley_general_educacion.pdf> [Consulta: 14 de enero de 2017]

Protección de los Derechos de las Niñas, Niños y Adolescentes.[95] Este cuerpo legal es una norma de orden público, cuyos objetivos principales son el reconocer a las niñas, niños y adolescentes como titulares de derechos de acuerdo a los principios de universalidad, interdependencia, indivisibilidad y progresividad, garantizándoles el pleno ejercicio, respeto, protección y promoción de sus derechos humanos conforme a lo dispuesto en la Constitución Política de los Estados Unidos Mexicanos. Específicamente el artículo 13 de la citada ley dispone como uno de los derechos de niñas, niños y adolescentes, el derecho a la intimidad personal y familiar y a la protección de sus datos personales, señalando expresamente que no podrán ser objeto de injerencias arbitrarias e ilegales en su vida privada, su familia, su domicilio o correspondencia; se considerará vulneración a la intimidad de este grupo de individuos, cualquier manejo de su imagen, nombre, datos personales o referencias que permitan su identificación en los medios de comunicación que cuenten con concesión para prestar el servicio de radiodifusión y telecomunicaciones, así como medios impresos, o en medios electrónicos de los que tenga control el concesionario o medio impreso de que se trate, que menoscabe su honra o reputación, sea contrario a sus derechos o que los ponga en riesgo conforme al principio de interés superior de la niñez. En lo que

[95] LEY GENERAL DE DERECHOS DE NIÑAS, NIÑOS Y ADOLESCENTES. México. Nueva Ley publicada en el Diario Oficial de la Federación el 04 de diciembre de 2014. Secretaría de Educación Pública. [En línea] < http://www.diputados.gob.mx/LeyesBiblio/pdf/LGDNNA_041214.pdf > [Consulta: 14 de enero de 2017]

respecta al consentimiento la norma alude a los medios de comunicación, estableciendo que en caso de difundir entrevistas a niñas, niños y adolescentes deberá recabar el consentimiento por escrito o por cualquier otro medio de quienes ejerzan la patria potestad o tutela, así como la opinión de ellos y en caso de que ello no sea posible, éste podrá otorgarlo siempre que ello no implique una afectación a su derecho a la privacidad por el menoscabo a su honra o reputación.

Por su parte, la norma citada se vincula – en este tema – con el Código Civil Federal de los Estados Unidos Mexicanos, el que señala que la mayoría de edad comienza a los 18 años, por tanto sólo a partir de esa edad y al igual que ocurre en nuestro país, será considerado plenamente capaz, pudiendo determinar por sí el tratamiento o la entrega de información que refiera a su persona, sin necesidad de representación de sus padres o de quien lo tenga a su cuidado, pues sólo al ser mayor de edad el individuo está habilitado legalmente para disponer de su persona y de sus bienes.[96]

[96] Artículos 646 y 647 del Código Civil Federal Mexicano.

2.b.4) Mantenimiento y actualización de datos personales de alumnos

En lo relativo al mantenimiento y actualización de los datos, cabe indicar que aquellos recogidos directamente del afectado o interesado – alumnos o sus padres y/o apoderados - se considerarán exactos; por tanto, los establecimientos educativos deben permanentemente actualizarlos y cancelarlos cuando queden obsoletos o no tengan ya ninguna finalidad. No será posible denegar la actualización de los datos por motivos de complejidad o volumen de la información almacenada.

La única referencia a este respecto en nuestra Ley, la encontramos en el artículo 6 inciso primero, al indicar que los datos personales deberán ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal o hayan caducado, la que se condice con las normas internacionales; en consecuencia, los establecimientos deberán realizar permanentemente revisiones de los datos para de esta manera actualizarlos correctamente, lo que implica:

- Tener procedimientos individualizados de actualización a petición de los interesados, así como procedimientos masivos periódicos de actualización y cancelación de los datos que mantengan la información actualizada.

- Cuando se modifiquen o se supriman ficheros de datos de carácter personal, esa modificación o supresión deberá declararse de la misma forma que se declaró su creación.
- Los datos serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados y el fichero deberá ser suprimido.

Por su parte, en cualquier fase del tratamiento, las personas que utilizan los datos de carácter personal están obligadas a la confidencialidad, es decir, no podrán revelar la información a terceros; deber de secreto que debe ser conocido por todas las personas de la organización educacional que tratan o utilizan datos de carácter personal.[97] Lo anterior en cumplimiento del artículo 11 de la Ley N° 19.628.

[97] Se trata de un deber distinto al deber de secreto de tipo deontológico que incumbe a algunos profesionales concretos (médicos, asistentes sociales, etc.) y – a su vez – perfectamente compatible con el mismo. En este sentido la legislación española ha considerado establecer para conocimiento de los trabajadores de los centros públicos de enseñanza la introducción en los contratos de trabajo o de prestación de servicios personales, cláusulas de confidencialidad. Además, el responsable del fichero o tratamiento está obligado a proporcionar a su personal que trate datos de carácter personal formación al respecto.

2.b.5) Obligación de garantizar la protección de antecedentes personales de menores en los contratos con terceros ajenos a la institución pública de educación

En el ámbito de la educación, normalmente los establecimientos educacionales contratan o acuerdan mediante convenio con terceros la prestación de determinados servicios que requieren el tratamiento de datos de carácter personal y que pueden afectar al tratamiento de los datos de toda la comunidad escolar; por ejemplo la agencia de viajes al organizar una actividad fuera del establecimiento; los servicios de alimentación, donde pueden existir datos relativos a alumnos alérgicos a determinados alimentos, entre otros servicios que comprenden la transmisión de datos personales a terceros que tratarán con ellos, debiendo mantenerse por tanto el debido resguardo. Siendo así este escenario, es obligación del centro de educación responsable del fichero garantizar que los contratos firmados con el personal, ya sea interno o perteneciente a una entidad externa con la que se contratan los servicios, aunque no tenga acceso habitual a datos de carácter personal de los alumnos, recojan las garantías precisas sobre el tratamiento de datos de carácter personal recogidos en sus ficheros.[98]

[98] En España, cuando se contrata la limpieza o mantenimiento de las instalaciones del centro docente u organismo de la Consejería con una empresa, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la

El caso de España, y como hemos venido señalando, es distinto. A estos efectos, la AEPD propone la utilización o adaptación al caso concreto de cláusulas tipo que permitirán resguardar pertinentemente los datos personales. A modo de ejemplo:

- “El/los adjudicatario/s declaran expresamente que conoce/n quedar obligado/s al cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. El/los adjudicatario/s se comprometen explícitamente a formar e informar a su personal en las obligaciones que de tales normas dimanan.”
- “La empresa adjudicataria declara expresamente que conoce quedar obligada al cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, y expresamente, en lo indicado en su artículo 10, en cuanto al deber de secreto…”
- “La empresa adjudicataria y el personal encargado de la realización de las tareas guardará secreto profesional sobre todas las informaciones, documentos y asuntos a los que tenga acceso o conocimiento durante la vigencia del contrato, estando obligado a no hacer públicos o enajenar cuantos datos conozcan como consecuencia o con ocasión de su ejecución, incluso después de finalizar el plazo contractual.”
- “Si la empresa adjudicataria aporta equipos informáticos, una vez finalizadas las tareas, previamente a retirar los equipos informáticos, deberá borrar toda la

---

prestación del servicio. Señala además la normativa que es conveniente la introducción de una cláusula por la que la empresa adjudicataria se comprometa, a su vez, a exigir a sus trabajadores la firma de una cláusula en sus respectivos contratos de trabajo.

información utilizada o que se derive de la ejecución del contrato, mediante el procedimiento técnico adecuado. La destrucción de la documentación de apoyo, si no se considerara indispensable, se efectuará mediante máquina destructora de papel o cualquier otro medio que garantice la ilegibilidad, efectuándose esta operación en el lugar donde se realicen los trabajos."

Por su parte, el RDLOPD contempla la posibilidad de subcontratación de un servicio con un tercero por parte del encargado de tratamiento, la que se podrá llevar a cabo cuando el encargado del tratamiento hubiera obtenido autorización del responsable del fichero, la que se efectuará siempre en nombre y por cuenta del responsable del fichero.[99] No será necesaria autorización del responsable del fichero si cumple los siguientes requisitos: 1) Que se especifiquen en el contrato los servicios que pueden ser objeto de subcontratación y la empresa con la que se vaya a subcontratar; 2) Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero; y 3) Que el encargado del tratamiento y la empresa formalicen el contrato en los términos previstos en las relaciones entre el responsable y el encargado del tratamiento.

[99] Artículo 21 del Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos, España.

Es por ello que el centro educativo responsable del fichero deberá también comunicar a la Agencia de Protección de Datos de España cualquier contrato que celebre y que incluya el tratamiento de datos de carácter personal de alumnos por parte de un tercero, con anterioridad a la firma del mismo,[100] atendido el carácter de los datos personales y la importancia de mantener su resguardo, garantía y protección.

En el caso mexicano, el Reglamento de la LFPDPPP[101] dispone en su artículo 54 que toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Agrega que una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido, asumiendo la persona física o moral subcontratada las mismas obligaciones que se establezcan para el encargado en la Ley, en el Reglamento y demás disposiciones aplicables. En cuanto a la autorización de la subcontratación, el artículo 55 del referido Reglamento señala que cuando las cláusulas contractuales o los instrumentos jurídicos mediante los cuales se haya formalizado la relación entre el responsable y el encargado, prevean que este último pueda llevar a cabo a su

[100] AGENCIA DE PROTECCIÓN DE DATOS de la Comunidad de Madrid, Op. Cit. Pág. 169.

[101] Nuevo Reglamento publicado en el Diario Oficial de la Federación el 21 de diciembre de 2011.

vez las subcontrataciones de servicios, la autorización antes mencionada se entenderá como otorgada a través de lo estipulado en éstos. En caso de que la subcontratación no haya sido prevista en las cláusulas contractuales o en los instrumentos jurídicos antes mencionados, el encargado deberá obtener la autorización correspondiente del responsable previo a la subcontratación.

3) Derechos de los titulares sobre sus datos personales

En aquellos países que el derecho a la protección de datos es considerado como derecho fundamental, su contenido incluye un haz de garantías y facultades que se traducen en determinadas obligaciones de hacer. Se habla entonces del derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelarlos,[102] derechos que por supuesto ostentan alumnos, padre y/o apoderados de establecimientos educacionales, surgiendo así los derechos ARCO – sigla para individualizar los derechos de Acceso, Rectificación, Cancelación y Oposición -, pilar fundamental en que se sustenta la garantía de

[102] MARTÍNEZ, R., 2007. El derecho fundamental a la protección de datos: perspectivas. Monográfico: III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas». Revista de Internet, Derecho y Política, España. Pág. 50. [En línea] <http://www.uoc.edu/idp/5/dt/esp/martinez.html> [Consulta: 29 de septiembre de 2016]

los datos personales, pues a través de ellos podrá hacerse efectiva su protección y amparo.

3.a) Derecho de Acceso

En términos generales, los titulares de los datos personales tienen derecho de acceder a su información personal que esté en posesión de terceros, para saber cuáles son y el estado en que se encuentran o los fines para los que se utilizan, conociendo así las características generales del uso al que están sometidos los datos personales. Se constituye como la puerta de entrada al ejercicio de los demás derechos, pues sólo si se tiene conocimiento o información sobre si se están tratando los datos y de qué manera se está haciendo, será posible conocer si se está respetando el principio de calidad y finalidad en el tratamiento, siendo posible exigir su eliminación, cancelación o bloqueo.[103]

Entre la información a la que puede accederse se encuentra, por ejemplo, los datos personales que usan los establecimientos públicos de educación; las finalidades que persiguen con su utilización; acceso a conocer quién utiliza los

[103] CENTRO DE ESTUDIOS DE DERECHO INFORMÁTICO. 2003. Derechos del Titular de Datos y Habeas data en la Ley 19.628, Revista Chilena de Derecho Informático, Facultad de Derecho, Universidad de Chile, ISNN 0717-9162. N° 2, Año 2003, Chile. [En línea]: <http://web.uchile.cl/vignette/derechoinformatico/CDA/der_informatico_simple/0,1493,SCID%253D14180%2526ISID%253D292%2526PRT%253D14178,00.html> [Consulta: 29 de septiembre de 2016]

datos personales; a saber con quiénes se comparte información personal y para qué fines; antecedentes relativos a qué datos personales se comparten con terceros; y de qué fuente se obtuvieron los datos personales, entre otros.[104]

En el caso chileno, el artículo 12 de la Ley N° 19.628 reconoce este derecho y además establece un procedimiento a su respecto, disponiendo que el responsable del fichero deberá resolver sobre lo solicitado en el plazo de dos días hábiles contado desde la recepción de la solicitud.[105] Si transcurrido dicho plazo, la solicitud no ha sido atendida adecuadamente, el interesado podrá dirigirse al juez de letras en lo civil del domicilio del responsable, que se encuentre de turno según las reglas correspondientes, solicitando amparo a su derecho de acceso consagrado en el artículo 16 de la ley citada.

Por su parte, el artículo 14 del cuerpo legal en comento ha dispuesto una norma especial para los organismos públicos en relación al ejercicio de derecho de información, señalando que: "*Si los datos personales están en un banco de datos al cual tienen acceso diversos organismos, el titular puede requerir*

[104] INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS. Guía práctica para ejercer el Derecho a la Protección de Datos Personales. [En línea] <http://inicio.ifai.org.mx/Publicaciones/01GuiaPracticaEjercerelDerecho.pdf> [Consulta: 29 de agosto de 2016]

[105] Artículo 16 Ley N° 19.628 sobre Protección de la Vida Privada: "*Si el responsable del registro o banco de datos no se pronunciare sobre la solicitud del requirente dentro de dos días hábiles…"*

información a cualquiera de ellos". Refiere la norma a bases de datos que son "compartidas" por distintos órganos públicos, en el caso que nos ocupa, y a modo de ejemplo, bases de datos que comparten instituciones como las Corporaciones Municipales de Educación, el Ministerio de Educación, la Superintendencia de Educación, entre otros, pudiendo recurrirse a cualquiera de ellas – independiente y paralelamente – con el objetivo de obtener la información relativa a datos personales,[106] el que en caso de niñas, niños y adolescentes deberá ser ejercido por padres o quien lo represente.

En México, el Reglamento de LFPDPPP señala que el titular de los datos tiene derecho a obtener del responsable de éstos la información relativa a las condiciones y generalidades del tratamiento,[107] casos en que el derecho se tendrá por cumplido cuando el responsable ponga a disposición del titular los datos personales en sitio, respetando el período de quince días de consulta, o bien a través de la expedición de copias físicas,[108] siempre que sean en formatos legibles o comprensibles para el titular. Sin perjuicio de lo anterior, es

[106] CENTRO DE ESTUDIOS DE DERECHO INFORMÁTICO, Op. Cit.

[107] Artículo 101, Reglamento de Ley Federal de Protección de Datos Personales en Posesión de Particulares. México.

[108] Puede ser además medios magnéticos, ópticos, sonoros, visuales u holográficos, o utilizando otras tecnologías de la información que se hayan previsto en el aviso de privacidad.

posible acordar medios de reproducción de la información distintos a los informados en el aviso de privacidad.[109]

España ha dispuesto que su ejercicio es personalísimo; en consecuencia, sólo podrá accederse a la información pretendida si se trata de información sobre datos personales propios, mas no de información de terceros, y en caso de ejercerlo, el responsable del fichero deberá resolver sobre lo solicitado en el plazo de un mes desde la recepción de la solicitud; y aun cuando no disponga de ella. Si transcurrido dicho plazo, la solicitud no ha sido atendida adecuadamente, el interesado podrá dirigirse a la Agencia con copia de la solicitud cursada y de la contestación recibida (si existiera), para que ésta a su vez se dirija a la oficina designada con el objetivo de hacer efectivo el ejercicio de ese derecho. Este derecho de acceso no puede ser ejercido en intervalos inferiores a doce meses, salvo que se acredite un interés legítimo.[110]

En cuanto a la forma de obtener la información solicitada en virtud del ejercicio de este derecho, ésta podrá ser a través de uno o varios de los siguientes sistemas de consulta del fichero: a) Visualización en pantalla; b) Escrito, copia o fotocopia remitida por correo, certificado o no; c) Correo

[109] Artículo 102, Reglamento de Ley Federal de Protección de Datos Personales en Posesión de Particulares. México.

[110] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Canal del responsable de ficheros, Op. Cit.

electrónico u otros sistemas de comunicación electrónicas; d) Cualquier otro sistema que sea adecuado a la configuración o implantación material del fichero o a la naturaleza del tratamiento, ofrecido por el responsable.[111]

En cuanto a la forma de ejercer este derecho, cabe señalar que en algunos actos personalísimos la intervención del tutor no será necesaria, mientras que en otras podrá ser necesaria pero desde luego no suficiente, ya que el tutelado tendrá que consentir para que el acto sea válido jurídicamente. Por su parte, en el supuesto de que la persona incapacitada no tuviera la capacidad legal suficiente para realizar determinados actos personalísimos, el tutor, como regla general, no podrá realizarlos por sí solo atendido el carácter de íntimos que éstos poseen; por lo tanto serían de imposible realización.[112] En atención a lo anterior, en Chile este derecho de acceso es de ejercicio personal según se infiere del artículo 12 de la Ley N° 19.628, pudiendo en estos casos ser los

[111] ESCUELA DE FORMACIÓN E INNOVACIÓN Y ADMINISTRACIÓN PÚBLICA. 2015 Protección de Datos de carácter Personal: Disposiciones Generales. Datos Especialmente Protegidos. Región de Murcia. Conserjería de Hacienda y Administración Pública, España. Pág. 23. [En línea] < https://webcache.googleusercontent.com/search?q=cache:sPZpfmsaD24J:https://efiapmurcia.carm.es/web/integra.servlets.Blob%3FARCHIVO%3DC1%2520TEMA%25208.pdf%26TABLA%3DARCHIVOS%26CAMPOCLAVE%3DIDARCHIVO%26VALORCLAVE%3D117853%26CAMPOIMAGEN%3DARCHIVO%26IDTIPO%3D60%26RASTRO%3Dc%24m2813,51996,51997+&cd=3&hl=es&ct=clnk&gl=es.> [Consulta: 30 de agosto de 2016]

[112] ASOCIACIÓN DE NIÑOS Y JÓVENES CON DISCAPACIDAD DE ALICANTE. ESCUELA DE FORMACIÓN E INNOVACIÓN Y ADMINISTRACIÓN PÚBLICA. 2015. Los Derechos Personalísimos. Departamento de Trabajo Social, Programa Gris “Protección Social y Acción Tutelar. Pág. 1 [En línea] < http://www.andalicante.org/enlaces/articulos-profesionales-anda/dossier-derechos-personalisimos.pdf .> [Consulta: 30 de mayo de 2017]

padres o tutores, en representación del hijo (a) menor de edad, quien ejerza el derecho de acceso bajo el amparo de la ley.

Así entonces, en casos de establecimientos educativos, el alumno – por si o representado por sus padres o apoderados - podrá ejercer su derecho de acceso a sus propios antecedentes, esto es, podrá requerir la entrega de su ficha personal, sus antecedentes académicos, sus antecedentes relativo a evaluaciones psicopedagógicas y todo otro dato personal que obre en poder de la institución de educación, ejerciendo de esta manera su derecho a conocer éstos, amén del origen de los datos, la finalidad para la cual se tratan, el uso que se le darán, los eventuales cesionarios de la misma y las comunicaciones de los mismos que se hayan realizados por el colegio; escenario en el que el centro educativo sólo podrá negarse, argumentando causales expresamente establecidas en la ley.

3.b) Derecho de Rectificación

Facultad referida a la posibilidad que tiene de todo titular de datos para solicitar la rectificación de aquellos que le conciernen, cuando éstos sean erróneos, inexactos, equívocos o incompletos. En estos casos la legislación

chilena exige, como requisito que se acredite por parte del titular de los datos la "mala calidad" del dato que se reclama.[113]

El artículo 12 de la Ley N° 19.628 establece el derecho a la rectificación de los datos personales, disponiendo que toda persona tiene derecho a exigir, a quien sea responsable de un banco, que se dedique en forma pública o privada al tratamiento de datos personales, que en caso que estos sean erróneos, inexactos, equívocos o incompletos, y así se acredite, su modificación, su eliminación o bloqueo; procedimiento gratuito que obliga al proporcionar, a solicitud del titular, copia del registro alterado en la parte pertinente. En caso de nuevas modificaciones o eliminaciones de datos, el titular podrá obtener sin costo copia del registro actualizado,[114] siempre que desde la precedente oportunidad que haya ejercido este derecho hayan transcurrido seis meses.

En la legislación mexicana el sentido de la norma es muy similar al caso chileno, disponiendo que el titular de los datos personales podrá solicitar en todo momento al responsable que rectifique sus datos personales que resulten ser inexactos o incompletos; para ello deberá indicar a qué datos personales se refiere, así como la corrección que haya de realizarse, acompañando la

[113] CENTRO DE ESTUDIOS DE DERECHO INFORMÁTICO, Op. Cit.

[114] Dispone la norma que el derecho a obtener copia gratuita de las partidas alteradas, o eliminadas sólo podrá ejercerse personalmente. Lo anterior no obsta a que tal actuación se pueda llevar a cabo a través de un mandatario habilitado legalmente para estos efectos.

documentación que ampare la procedencia de lo solicitado. Por su parte, se insta al responsable del tratamiento a ofrecer mecanismos que faciliten el ejercicio de este derecho en beneficio del titular, disponiendo de 20 días para dar respuesta al requerimiento.[115]

En el caso español, su concepto se asemeja al de nuestro país. La AEPD ha señalado que éste es uno de los derechos que la LOPD reconoce a los ciudadanos para que puedan defender su privacidad controlando por sí mismo el uso que se hace de sus datos personales, y en particular, el derecho a que éstos se modifiquen cuando resulten inexactos o incompletos. Su ejercicio es personalísimo, por ende, sólo es posible que lo solicite la persona interesada, quién deberá dirigirse al ente privado o al organismo público – escuelas públicas - que sabe o presume que tiene sus datos, indicando a cuáles de ellos se refiere, la corrección que se solicita, y aportando al efecto la documentación que lo justifique. Ante tal presentación el responsable del fichero deberá resolver sobre lo solicitado en el plazo máximo de diez días a contar desde la recepción de la solicitud, debiendo hacerlo también aunque no disponga de datos del afectado. Transcurrido el plazo sin que de forma expresa se responda a la petición o ésta sea insatisfactoria, el interesado podrá reclamar tutela a su derecho ante la AEPD, acompañando la documentación que acredite haber solicitado la rectificación de datos ante la entidad de que se trate.

[115] Artículo 32, Ley Federal de Protección de Datos Personales en Posesión de Particulares.

En casos de colegios, los alumnos tienen la facultad de ejercer este derecho solicitando expresamente que se rectifiquen los datos inexactos relativos a su persona. A modo de ejemplo, puede solicitarse la rectificación del domicilio del alumno, su número telefónico de contacto o bien la rectificación de alguna situación que afecte su salud (ingesta de medicamentos, tratamientos a realizar durante la jornada escolar, etc.), sus hábitos alimenticios u otros; requerimientos que debe ser satisfecho por la entidad educativa en los plazos que cada ley disponga a tales efectos.

3.c) Derecho de Cancelación

Este derecho se constituye como la facultad de todo titular de datos para exigir la destrucción de los datos almacenados, cualquiera fuere el procedimiento empleado para ello, cuando este almacenamiento carezca de fundamento legal o cuando estuvieran caducos.

A este respecto es preciso señalar que la eliminación de los datos personales no siempre procede de manera inmediata, pues a veces es necesaria la conservación de los mismos con fines legales, de responsabilidades o contractuales, período al que la Ley denomina *bloqueo*, no pudiendo utilizarse los datos personales para ninguna finalidad, y una vez concluido deberán ser eliminados.

La cancelación o eliminación de datos personales procederá, en el caso chileno, cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado, de conformidad a lo dispuesto por el artículo 6, inciso primero de la Ley Nº 19.628,[116] agregando que se bloquearán los datos personales cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa y respecto de los cuales no corresponda cancelación; el responsable del banco de datos personales procederá a la eliminación, modificación o bloqueo de los datos, en su caso, sin necesidad del requerimiento del titular.

En México, este derecho a cancelación implica el cese en el tratamiento por parte del responsable, a partir del bloqueo de los mismos y su posterior supresión, pudiendo el titular de los datos en todo momento solicitar al responsable la cancelación de los datos personales cuando considere que los mismos no están siendo tratados conforme a los principios y deberes que establece la Ley y el Reglamento mexicano, procediendo la cancelación respecto de la totalidad de los datos personales del titular contenidos en una base de datos, o sólo parte de ellos, según lo haya solicitado.[117]

[116] Artículo 6, inciso primero de la Ley N° 19.628: "*Los datos personales deberán ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado…"*

[117] Artículos 105 y 106 del Reglamento de Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

En cuanto al límite del derecho a cancelación, cabe advertir que no se constituye como derecho absoluto, sino que encuentra sus restricciones en la eficacia de los otros derechos fundamentales, entre los que se encuentra el derecho a la educación. Consecuentemente con lo anterior, será el responsable del registro del establecimiento educacional quien deba garantizar la prestación educativa salvaguardando el interés general, motivo por el que existe el límite a la cancelación de historiales académicos, lo que no ocurre por ejemplo, con los expedientes de atención psicopedagógica de un alumno, respecto de los cuales es posible su cancelación al finalizar el proceso educativo.[118] Misma situación respecto de fotografías de alumnos que se encuentren en sitios webs por realización de actividades extracurriculares, en las que debe atenderse el derecho a la imagen del menor, pudiendo los padres solicitar la cancelación de ese dato de los registros que posea el establecimiento educativo.

A nivel internacional en lo referido a la cancelación, ésta implica el bloqueo de los datos, los que se mantienen únicamente a disposición de la Administración Pública y de los tribunales de justicia, debiendo ser borrados cuando finalice el plazo de prescripción de las responsabilidades originadas del

[118] AGENCIA DE PROTECCIÓN DE DATOS de la Comunidad de Madrid, Op. Cit. Pág. 86.

tratamiento de datos; Ana Herrán Ortíz señala que, cumplido el plazo de prescripción deberá procederse a la supresión del dato en cuestión.[119]

Específicamente en España, el plazo para pronunciarse por este derecho, es de 10 días.

3.d) Derecho de Bloqueo

El derecho de bloqueo, según la ley chilena, consiste en aquella facultad que le corresponde a todo titular de datos para exigir la suspensión temporal de cualquiera de las operaciones del tratamiento de datos, procediendo en todos aquellos casos en que la exactitud de los datos no pueda ser establecida o su vigencia sea dudosa y respecto de los cuales no corresponda la cancelación; en la práctica este derecho se traduce en la imposibilidad de comunicar el dato bloqueado a terceros.

Su fundamento legal radica en el artículo 3 inciso final de la Ley Nº 19.628, que al tenor señala: *"El titular puede oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado o encuestas de*

[119] HERRÁN, A., 2002. El derecho a la intimidad en la nueva Ley orgánica de protección de datos personales. Editorial Dykinson. Madrid, España. Página 255. [En línea] <https://books.google.cl/books?id=CCVT48egc5MC&pg=PA256&lpg=PA256&dq=derecho+a+bloqueo+de+datos+personales+en+la+ley+espa%C3%B1ola&source=bl&ots=qTTMFk2TGu&sig=IWYxZcsk7bf4sre7hdI_OdYe7IY&hl=en&sa=X&ved=0ahUKEwiqhMnQ3sPLAhVEjJAKHXpLB7sQ6AEILDAD#v=onepage&q=derecho%20a%20bloqueo%20de%20datos%20personales%20en%20la%20ley%20espa%C3%B1ola&f=false> [Consulta: 01 de julio de 2016]

opinión"; además esta oposición podrá ejercerse en cualquier etapa del tratamiento de los datos, ya sea en su recogida, almacenamiento, transferencia, etc. [120]

A este respecto el artículo 12 inciso cuarto de la Ley N° 19.628 dispone que: *"Igual exigencia de eliminación, o la de bloqueo de los datos, en su caso, podrá hacer cuando haya proporcionado voluntariamente sus datos personales o ellos se usen para comunicaciones comerciales y no desee continuar figurando en el registro respectivo, sea de modo definitivo o temporal"*. Para el caso de los colegios, ejemplo de derecho a bloqueo pueden ser la cancelación de tratamiento de datos personales entregados por los padres y/o apoderados (alumnos), para invitaciones a talleres o actividades extra-programáticas del establecimiento. La citada norma, a falta de precepto legal que regule la materia en forma expresa, puede servir de base para oponerse en sede extrajudicial al denominado "spam" o correo electrónico no deseado, atendido a que en éste se utilizan datos personales precisamente con fines de publicidad, cuando los padres o apoderados de los alumnos (menores de edad), no deseen continuar recibiendo información (invitaciones /spam) por parte del centro educativo.

Tomando el ejemplo comparado, y de acuerdo a lo establecido en la legislación española, este derecho de oposición podrá ser ejercitado cuando no sea necesario para su tratamiento el consentimiento del interesado, como

[120] CENTRO DE ESTUDIOS DE DERECHO INFORMÁTICO, Op. Cit.

consecuencia de un motivo legítimo y fundado, justificado en una concreta situación personal y siempre que la ley no disponga lo contrario. A este respecto, el Real Decreto 1720/2007 español[121] establece los siguientes supuestos en los que se debe fundamentar el derecho de oposición del afectado:[122] a) Cuando se trate de registros que tengan por finalidad la realización de actividades de publicidad y prospección comercial; b) Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal. En este contexto, será posible ejercer este derecho a no verse sometido a una decisión con efectos jurídicos sobre ellos o bien, que les afecte significativamente, basada únicamente en un tratamiento automatizado de datos destinados a evaluar determinados aspectos de su personalidad.[123]

Este derecho de oposición se ejercerá mediante una solicitud dirigida al responsable del fichero, debiendo cumplir los mismos requisitos que en caso del derecho de acceso; en aquellos casos en que la oposición se realice en base a los supuestos que contempla la LOPD, la solicitud deberá constar los motivos fundados y legítimos en relación a una concreta situación personal del afectado que justificarán el ejercicio de este derecho. Frente a este escenario,

[121] Artículo 34.

[122] AGENCIA DE PROTECCIÓN DE DATOS de la Comunidad de Madrid, Op. Cit. Pág. 453.

[123] Tales como rendimiento laboral, créditos, fiabilidad o conducta, entre otros.

el responsable del registro o fichero resolverá sobre la solicitud de oposición en un plazo máximo de diez días contados desde que se recepciona la solicitud;[124] si transcurre el plazo sin que se notifique expresamente la respuesta a ésta, se entenderá desestimada pudiendo el afectado presentar una reclamación ante la Autoridad de Control de Protección de Datos competente.

En caso de no disponer de datos de carácter personal de los afectados deberá comunicar esta situación en el mismo plazo de diez días; además el responsable del fichero debe excluir del tratamiento de los datos relativos al afectado que ejercite su derecho de oposición o denegar fundadamente la solicitud del interesado en el plazo indicado.

En nuestro país, en el ámbito escolar, para aquellos casos en que se solicite al responsable del registro o banco de datos la modificación, eliminación o bloqueo de éstos y aquel no se pronunciare sobre la solicitud del requirente en el plazo de dos días hábiles, o la denegare por causas distintas a la seguridad de la Nación o en interés nacional, nace para el titular de los datos el derecho a recurrir ante el juez de letras en lo civil del domicilio del responsable, solicitando el amparo de estos derechos, diligencias que podrán ser gestionadas por el padre o la madre (o apoderado), respecto de los datos del hijo/a o pupilo/a menor de edad, entregados al establecimiento de educación.

[124] Artículo 35 del Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos Personales, España.

De acuerdo al artículo 13 de la ley en comento, los derechos de las personas a la información, modificación, cancelación o bloqueo de sus datos personales no podrá ser limitado por medio de ningún acto o convención; sin perjuicio de ello no podrá solicitarse información, modificación, cancelación o bloqueo de datos personales cuando ello impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del órgano público requerido, o cuando afecte la reserva o secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la Nación o el interés nacional; tampoco será posible solicitar la modificación, cancelación o bloqueo de datos personales almacenados por mandato legal, fuera de los casos contemplados en la ley respectiva; ello de conformidad a lo dispuesto en el artículo 15 de la Ley Nº 19.628.

Finalmente, es posible afirmar que el ejercicio de los derechos de acceso, rectificación, cancelación y bloqueo de datos personales en establecimientos educacionales – públicos y también privados - no es muy alto y la razón de ello sea probablemente por la falta de conciencia de los menores y, básicamente, de sus padres, representantes legales o apoderados acerca de la importancia que reviste el ejercicio de tales derechos en pro de la protección de sus datos personales.

En virtud de lo expuesto es menester que los colegios garanticen el principio de información de acuerdo a lo dispuesto en los artículos 3, 4, 5 y 12 de la Ley

Nº 19.628, informando en la recogida de datos sobre la existencia del registro, la finalidad de éste, los posibles cesionarios, la identidad y dirección del responsable de los mismos, para que de esta manera los derechos ARCO puedan ser efectiva y eficazmente ejercidos y protegidos.

CAPÍTULO TERCERO

ÁMBITO DE APLICACIÓN DE LA LEY N° 19.628 SOBRE PROTECCIÓN DE LA VIDA PRIVADA Y PRINCIPIOS DE LA PROTECCIÓN DE DATOS PERSONALES APLICADOS AL SECTOR EDUCACIÓN

1) Contexto

Cuando hablamos de protección de datos, nos referimos al reconocimiento que el ordenamiento jurídico realiza respecto del individuo, como titular de los derechos que, constitucional o legalmente, el sistema normativo ampara y garantiza. En virtud de tal declaración, se faculta a las personas a controlar sus datos personales, otorgándole una serie de derechos que en definitiva se traducen en la capacidad que tiene éste para disponer, informarse y decidir sobre aquellos.

Actualmente la tecnología en este tema va de la mano con la protección de datos, unión que en pleno siglo XXI es casi indisoluble, pues los progresos en la era digital y la tecnología cada día más avanzada permiten que en cada actuar en sociedad el ciudadano – el individuo – deje huellas, las que posteriormente

podrán ser recogidas y, eventualmente, tratadas por otros, donde resulta del todo importante ponderar entre derecho del individuo a preservar el control sobre sus datos personales y la aplicación de las nuevas tecnologías de la información,[125] como un derecho de tercera generación que requiere garantías que lo hagan impermeable a la intromisión de personas naturales y/o personas jurídicas sin la debida autorización,[126] con el objetivo de preservar la identidad, la dignidad y la libertad. Surge entonces el derecho del individuo a "quedarse solo" y la "autodeterminación informativa";[127] concepto que sigue los derroteros propios de los derechos fundamentales de nueva generación que surgen a raíz de la "*liberties pollution*"[128] de las categorías precedentes, y que se abrió paso tímidamente entre la doctrina y jurisprudencia nacionales, para finalmente

[125] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía del Responsable del Fichero: Guía de Protección de datos para Responsables de Ficheros. [En línea] <https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_responsable_ficheros.pdf> [Consulta: 28 de julio de 2016]

[126] La protección de datos como derecho de tercera generación, el que emerge a partir de la segunda mitad del siglo XX en el marco de la promoción del progreso social y calidad de vida de todos los pueblos en un marco de respeto y colaboración mutua entre las distintas naciones de la comunidad internacional.

[127] Se denomina autodeterminación informativa a la facultad que tiene toda persona para ejercer control sobre la información personal que le concierne, contenida en registros públicos o privados, especialmente los almacenados mediante medios informáticos, siendo considerado como Derecho de Tercera Generación.

[128] Fenómeno y concepto acuñado por Pérez Luño y conocido como "Contaminación de las libertades", la cual se ha derivado por el uso de las nuevas tecnologías; fenómeno es ocasionado por la aparición de nuevos derechos o por la redefinición de los ya existentes, pero que deben ser adaptados a los nuevos contextos que se presenten, como en este caso, el desarrollo de las nuevas tecnologías. En tal sentido, el individuo y su intimidad se convierten en un nuevo blanco de ataque, pero esta vez derivado por el uso y control de sus datos personales que en muchas ocasiones se lleva a cabo sin su consentimiento; en consecuencia, la exigencia de nuevos derechos es también exigencia de construcciones de nuevos conceptos, que tendrán en este caso como antecedente, la esfera íntima y al propio individuo y su protección.

cristalizar su reconocimiento en disposiciones legales, llegando a constitucionalizar su contenido e inclusive a recibir acogida en instrumentos internacionales.

Sin perjuicio de lo anterior, valga mencionar que el concepto de autodeterminación, atendidas las circunstancias de la vida contemporánea y la sociedad de redes, va quedando un poco atrás, dando lugar a otro denominado "expectativa de privacidad". Tal concepto se enmarca dentro del contexto de que no es posible obviar que la privacidad constantemente es amenazada por el desarrollo de la tecnología que facilita a cualquier persona adquirir información sobre otra que normalmente no podría conocer sin su autorización, batalla librada fecundamente en el siglo XX, traduciéndose en la lucha por adaptar los principios sobre privacidad a los constantes avances tecnológicos, donde subsiste la preocupación central por preservar el carácter privado o confidencial de la información que nos atañe, para de esta manera retener cierto control sobre su uso y diseminación.[129] En este sentido, se ha argumentado que la "privacidad de la información" está dada por una expectativa razonable de que, bajo circunstancias normales, la mayoría de la

[129] GONZÁLEZ, F., s.a. Privacidad de la Información digital: autodeterminación vs. Commodity. Revista Jurídica de la Universidad de Palermo, Argentina. Pág. 77. [En línea] < http://www.palermo.edu/derecho/publicaciones/pdfs/revista_juridica/Especiales_SELA/SELA%201998%20-%20Ed%201999/04SELA98Juridica07.pdf> [Consulta: 06 de enero de 2017]

información respecto a uno mismo no está disponible públicamente.[130] En virtud de lo anterior podríamos sostener que el derecho a la intimidad o privacidad frente a la actividad estatal tiene ciertos límites,[131] pues se presume la existencia de la expectativa razonable de privacidad, por medio de la cual, los titulares de los datos personales depositan su confianza en otra persona – o entidad – para que pueda llevar a cabo su tratamiento de conformidad a la Ley.[132]

En el contexto escolar es obligación que la información que se maneje por parte de la entidad educativa sea conservada y protegida de cualquier forma de intromisión, lo que se vincula directamente con esta expectativa de privacidad que tienen los padres o apoderados respecto de toda aquella información que entregan al momento de matricular a un menor a su cargo en el centro de educación y aquella proporcionada en el devenir del año escolar.

[130] Ibid, Pág. 90.

[131] GUTIÉRREZ, A., 2014. El Derecho a la intimidad en la era de la tecnología de las comunicaciones: Una reflexión desde el derecho constitucional. Cuestiones Constitucionales, Revista Mexicana de Derecho Constitucional, Num. 31. México. Página 1 [En línea] < http://www.scielo.org.mx/pdf/cconst/n31/n31a8.pdf> [Consulta: 07 de enero de 2017]

[132] PRIVACIDAD VS PUBLICIDAD DE LOS DATOS PERSONALES EN POSESIÓN DE AUTORIDADES. 2014. México. El Observatorio. [En línea] < http://oiprodat.com/2014/01/23/privacidad-vs-publicidad-de-los-datos-personales-en-posesion-de-autoridades/> [Consulta: 07 de enero de 2017]

2) El derecho a la protección de datos: Normativa chilena y su ámbito de aplicación

La normativa de protección de datos en nuestro país es una legislación joven, razón por la que es considerada aún inmadura y potencialmente modificable en muchas de sus aristas.

En cuanto a su ámbito de aplicación, debemos señalar que la Ley Nº 19.628 sobre Protección de la Vida Privada se dictó en el año 1999; su origen viene dado por el respeto de los derechos y libertades fundamentales de un individuo, motivo por el que – según la Historia de la Ley[133]- se legisla en tal sentido y específicamente sobre el respeto a la intimidad de la persona ante el cada vez más frecuente tratamiento automatizado de los datos de carácter personal en el escenario de la "*sociedad de la información*".

Es así que se dicta este cuerpo legal para reconocer ciertos derechos de los individuos y también para imponer responsabilidades a los titulares de la base de datos o fichero, en relación a: la recolección imparcial y legal de los datos; garantía de que la recopilación y el almacenamiento de los datos se realiza con una finalidad legítima y concreta, y que la información no se empleará con fines

[133] Véase Historia de la Ley, Biblioteca del Congreso Nacional. [En línea] <http://www.leychile.cl/Consulta/portada_hl?tipo_norma=XX1&nro_ley=19628&anio=2016> [Consulta: 14 de julio de 2016]

ajenos a los indicados; adecuación entre los objetivos a alcanzar con la configuración del fichero y el número y la calidad de los datos recopilados; exactitud de los datos y, cuando sea necesario, su actualización; régimen de recursos, sanciones y responsabilidades.[134]

Concretamente, la ley estableció en su artículo 1 como su ámbito de aplicación *"el tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares se sujetará a las disposiciones de esta ley",* disponiendo que serán considerados datos personales *"los relativos a cualquier información concerniente a personas naturales, identificadas o identificables*",[135] y datos sensibles ***"****aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual."*[136]

---

[134] ARAYA, A., 2012. La Ley 19.628 sobre protección de datos de carácter personal y el contrato de trabajo: ¿una nueva cláusula obligatoria?. Novoa & Araya, Serie notas y artículos de interés número 2, Chile. Pág. 3. [En línea] <http://www.nyaabogados.cl/docs/NotasyArticulosNA_N2_Ley%2019628.pdf> [Consulta: 15 de julio de 2016]

[135] Art. 2, letra f, Ley Nº 19.628.

[136] Art. 2, letra g, Ley Nº 19.628.

En este sentido la ley establece que todo tratamiento de datos personales "*sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello"*, debiendo la autorización del titular constar por escrito, pudiendo además ser libremente revocada también por escrito, aunque sin efecto retroactivo.[137]

En cuanto a los datos sensibles la ley es más exigente y dispone que, salvo que la ley lo autorice o exista el consentimiento del titular, tales datos no pueden ser objeto de tratamiento, con la excepción de casos en que el tratamiento de datos sensibles sea necesario para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.[138]

Además del derecho a que se solicite y obtenga la autorización previa y escrita del titular, éste tiene una serie de derechos adicionales – analizados en capítulo II -: (i) información respecto de qué datos sobre sí mismo se encuentran registrados;[139] (ii) que sus datos se eliminen o cancelen cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado; (iii) que se modifiquen, cuando sean erróneos, inexactos, equívocos o incompletos;

[137] Art. 4, Ley Nº 19.628.

[138] Art. 10, Ley Nº 19.628.

[139] Art. 12 Ley Nº 19.628.

(iv) que se bloqueen transitoriamente, cuando su vigencia sea dudosa,[140] y (v) que sólo se utilicen para el fin para el cual fueron recolectados,[141] derechos que son garantizados por una serie de recursos y que deben ser respetados por el responsable que administre la base de datos, quien deberá indemnizar por daños materiales y morales que pudiese causar en caso de incumplimiento.[142]

Atendido lo expuesto, es posible efectuar un análisis del ámbito de aplicación de la Ley Nº 19.628, en su aspecto material u objetivo por una parte, como en su aspecto subjetivo por la otra. A saber:

2.a) Ámbito de aplicación objetivo

El ámbito de aplicación material u objetivo de la Ley Nº 19.628 se encuentra regulado básicamente en su artículo 1º inciso 1º que indica "*El tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares se sujetará a las disposiciones de esta Ley*", precepto que se encuentra determinado por el concepto de tratamiento de datos personales, el que consiste, según artículo 2 letra o), en "*cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o*

[140] Numerales (ii) al (iv), Arts. 6 y 12 Ley Nº 19.628.

[141] Art. 9 Ley Nº 19.628.

[142] Art. 23 Ley Nº 19.628.

no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma", el que se describe como un concepto amplio y genérico dada la utilización del vocablo "*cualquier*" y de la frase "*o utilizarlos en cualquier otra forma"* que comprende diversas acciones de carácter técnico a título ilustrativo, amplitud de definición que conlleva a que la Ley se aplique a cualquier operación que permita utilizar datos personales de alguna forma, ya sea éste automatizado o manual.

Por su parte, este concepto de tratamiento de datos debemos relacionarlo necesariamente con el de registro o banco de datos, definido por la Ley en el artículo 2 letra m) como "*el conjunto organizado de datos de carácter personal, sea automatizado o no, y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos*.", pues necesariamente el tratamiento que realice el responsable – o el encargado, en su caso -, ya sea órgano público o privado, lo será respecto de bases o registro de datos.

De estos dos conceptos básicos queda de manifiesto el ámbito material de la Ley, el que resulta comprensivo tanto de las operaciones de tratamiento automatizado o manual de datos, estableciendo como elemento esencial la

circunstancia de que tal tratamiento permita relacionar los datos personales entre sí, conformando un conjunto organizado de ellos para su respectiva consulta.[143]

2.b) Ámbito de aplicación subjetivo

Ámbito referido a quiénes y en qué términos se les aplica la Ley Nº 19.628. De una parte, se encuentran aquellos que efectúan tratamiento de datos personales en registros o bancos de datos, los que según el artículo 1° inciso 1º de la ley en comento pueden ser particulares u organismos públicos; y por otra parte encontramos a los titulares de la información de naturaleza personal. Agregar que también existe otra categoría de persona que resulta regulada en la ley, es decir, la del tercero receptor de datos personales.

En este campo de acción nos encontramos con aquellos jardines infantiles, colegios municipalizados y liceos municipales, respecto de las cuales aplicaría este ámbito subjetivo, pues de acuerdo a sus competencias y atribuciones es de toda lógica que estos establecimientos educativos traten datos de sus alumnos como de su personal docente e inclusive de terceros, recolectando,

[143] JERVIS, P., 2006. Regulación del Mercado de Datos. Tesis para optar al grado de Magíster en Derecho. Facultad de Derecho, Escuela de Graduados, Universidad de Chile, Chile. Pág. 83. [En línea] <http://repositorio.uchile.cl/handle/2250/114258> [Consulta: 28 de julio de 2016]

organizando, cediendo o transfiriendo – entre otras acciones – éstos y para distintas finalidades.

2.b.1) Particulares dedicados al tratamiento de datos: Aquellos titulares de bancos o registros de datos que efectúan tratamiento de datos personales en forma particular o privada. La ley chilena permite que éstos sean personas naturales o jurídicas (misma situación que la legislaciones mexicana y española); por ende, los establecimientos educativos privados son instituciones particulares dedicadas a la labor educacional de los alumnos, a quienes también se les aplica la normativa en su dimensión subjetiva.

2.b.2) Organismos públicos dedicados al tratamiento de datos: Organismos públicos titulares de bancos o registros de datos que efectúan tratamiento de datos personales. El artículo 2 letra k) de la Ley en comento es de amplio alcance, comprendiendo a las autoridades, órganos del Estado y organismos descritos y regulados por la Constitución Política como los comprendidos en el inciso segundo del artículo 1º de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.[144] Se destaca que los organismos públicos que efectúan tratamiento de datos poseen una regulación

[144] Entre ellos: Ministerios, Intendencias, Gobernaciones y los órganos y servicios públicos creados para el cumplimiento de la función administrativa, incluidos la Contraloría General de la República, el Banco Central, las Fuerzas Armadas y las Fuerzas de Orden y Seguridad pública, los Gobiernos Regionales, las Municipalidades y las empresas públicas creadas por ley.

especial en la Ley, que se encuentra en su Título IV "*Del tratamiento de datos por organismos públicos*".[145]

En cuanto al responsable de la base de datos, el artículo 2 letra n) de la ley lo define como "*la persona natural o jurídica privada, o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento de los datos de carácter personal*"; en consecuencia resulta importante diferenciar entre los titulares de registros o bancos de datos –categoría que no se reconoce en forma expresa en la ley- y los responsables del registro o banco de datos, distinción de género a especie, pues todos los responsables son titulares de registros o bancos de datos, ya que entendemos que efectúan tratamiento de datos ya sea en forma directa o a través de un tercero siendo esencial en todo caso que tomen las decisiones relacionadas con el tratamiento; no obstante, no todos los que tratan datos son responsables de los registros o bancos de datos, pues existen casos en que éstos no toman por sí las decisiones respecto al tratamiento que efectúan, por ejemplo puede ocurrir con los contratos de prestación de servicios de limpieza, de soporte informático, outsourcing, mandato para representación del establecimiento;[146] circunstancia en la que las

[145] Este Título consta de tres artículos: el 20 que establece los requisitos para que los organismos públicos puedan efectuar tratamiento de datos; el 21 que se refiere al tratamiento de datos de naturaleza penal o criminal que efectúan los organismos públicos; y, finalmente el 23, que regula el Registro de los bancos de datos que llevan organismos públicos, tarea encomendada por el mismo artículo al Servicio de Registro Civil e Identificación.

[146] Artículo 8 de la Ley Nº 19.628 permite que el tratamiento de datos se efectúe por mandato, en cuyo caso, se aplicarán las reglas generales. No obstante, establece que el mandato deberá

decisiones respecto del tratamiento no las toma el que lo efectúa sino el que lo encarga a través de contratos, esto es, el establecimiento de educación como responsable del tratamiento. (colegio municipal, la Superintendencia de Educación; y Ministerio de Educación u otro)

La distinción anterior tiene especial importancia en materia de responsabilidad por el tratamiento de datos regulada en la Ley, ya que conforme al artículo 23, será la persona natural o jurídica privada o el organismo público responsable del tratamiento de datos, quien deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos.[147]

2.b.3) El titular de los datos personales: Persona natural a la que se refieren los datos de carácter personal, que en el ámbito subjetivo aplicaría a todo el

---

ser otorgado por escrito, dejándose especial constancia de las condiciones de la utilización de los datos. El mandatario deberá respetar esas estipulaciones en el cumplimiento de su encargo.

[147] En el caso español, el artículo 45 de la Ley Orgánica de Protección de Datos establece las sanciones aplicables a los responsables del banco de datos y sobre éstas, especifica que la cuantía se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora, existiendo además un régimen específico en el caso de los ficheros de titularidad pública.
En el caso mexicano, el artículo 62 de la LPDPPP, refiere al "presunto infractor", entendiendo que este puede ser el titular del registro como también el responsable del mismo, sobre quienes se investigarán los hechos que motivaron el inicio del procedimiento, otorgándose un término de quince días para que se rinda pruebas y se manifieste por escrito lo que a sus derechos convengan.

universo de la comunidad escolar. Cabe señalar que nuestra legislación opta por no comprender a las personas jurídicas, como sí lo han hecho otros ordenamientos (como el argentino); pues nuestro legislador entiende que la intimidad, la vida privada son derechos que le corresponden en propiedad a las personas naturales y no a las jurídicas,[148] a las cuales se les puede proteger por otras vías, como por ejemplo, por vía de reserva o secreto.[149]

2.b.4) Terceros receptores de datos personales: Finalmente, una tercera categoría de personas que resulta normada indirectamente por la Ley Nº 19.628, son los terceros a los cuales se les comunican o transfieren datos personales. Si bien no existe una regulación orgánica en la ley con respecto a estos sujetos, el artículo 5 de la ley en comento que regula los procedimientos automatizados de transmisión o transferencia electrónica de datos personales se refiere a ellos cuando indica que la responsabilidad derivada de un requerimiento de datos personales mediante una red electrónica será de quien la haga, es decir, del tercero a quien se le comunican los datos, agregando que éste sólo podrá utilizar los datos personales para los fines que motivaron la

[148] A este respecto el Primer Informe de la Cámara de Diputados indicó que "En principio, el concepto de dato personal – y más aún el de intimidad - no es aplicable a las personas jurídicas y, por tanto, sus datos podrán ser siempre conocidos, pues prima el derecho a la información. Otra cosa será lo que se regule respecto del secreto comercial o industrial, por ejemplo". Informe de la Comisión de Constitución, Legislación y Justicia recaído en el proyecto de ley sobre protección a la vid a privada. Cámara de Diputados. Segundo Trámite. Sesión 3, pág. 152. 04 de junio de 1996.

[149] No obstante lo anterior, cabe consignar que han existido algunas iniciativas legales en orden a incorporar a las personas jurídicas dentro del ámbito de aplicación de la ley, así por ejemplo, el Boletín 2422-07.

transmisión; disposición que no será aplicable cuando se trate de datos personales accesibles al público en general o cuando se transmiten datos personales a organizaciones internacionales en cumplimiento de lo dispuesto en los tratados y convenios vigentes.

3) Principios de la Protección de Datos

Hemos señalado que la Ley chilena de protección de datos en ciertas hipótesis se presenta débil en lo que precisamente es su norte, requiriendo de ajustes y perfeccionamientos que ya se encuentran en trámite y que merecen acuciosidad y observancia en consideración a las implicancias que tales modificaciones puedan tener.

En este sentido, y sin perjuicio de la necesidad de perfeccionamiento de la Ley N° 19.628, los preceptos de la misma establecen un sistema que ha venido a ordenar el tratamiento de datos personales evitando, al menos, algunos abusos. No basta con que los derechos sean incorporados en la legislación, sino que también se hace necesario configurar un sistema complejo de protección de las personas que, junto con establecer normas, se sirva de ciertas consideraciones mínimas que deben ser incorporadas en las reglamentaciones sobre la materia, y que permita la implementación de mecanismos que tutelen la efectividad de su cumplimiento. Aparecen así, los principios informadores de

la Ley de Protección de Datos que han de inspirar la forma y la oportunidad en que se tratan los datos personales por parte de los responsables del mismo.

Estos principios además han sido establecidos por distintos organismos internacionales, tales como la Organización de Cooperación y Desarrollo Económicos – OCDE - a través de su "Recomendación relativa a las directrices aplicables a la protección de la vida privada y a los flujos transfronterizos de datos personales";[150]el Consejo de Europa con la "Recomendación de la Comisión 81/670/CEE relativa al Convenio del Consejo de Europa sobre protección de las personas con respecto al tratamiento automatizado de datos de carácter personal";[151] la Organización de las Naciones Unidas por medio de los "Principios rectores para la reglamentación de los ficheros computarizados de datos personales",[152] la que los dispone como directrices generales y flexibles en atención a que su propósito es su incorporación a las legislaciones internas de los países.[153]

---

[150] Adoptada por el Consejo de Ministros de esta organización el 23 de septiembre de 1980. [En línea] <http://www.oecd.org/sti/ieconomy/15590267.pdf> [Consulta: 09 de agosto de 2016]

[151] RECOMENDACIÓN DE LA COMISIÓN 81/670CEE de 29 de julio de 1981. [En línea] <https://www.boe.es/buscar/doc.php?id=BOE-A-1985-23447> [Consulta: 09 de agosto de 2016]

[152] PRINCIPIOS RECTORES PARA LA REGLAMENTACIÓN DE FICHEROS COMPUTARIZADOS DE DATOS PERSONALES, adoptado por la Asamblea General de las Naciones Unidas en su resolución 45/95 de 14 de diciembre de 1990. [En línea] <http://inicio.ifai.org.mx/Estudios/D.3BIS-cp--Directrices-de-Protecci-oo-n-de-Datos-de-la-ONU.pdf> [Consulta: 09 de agosto de 2016]

[153] JERVIS, Op. Cit. Pág. 62 y ss.

Importante es indicar que tales principios deben existir siempre estructurados y encontrarse presente en todo el ordenamiento jurídico de protección de datos: 1) Al momento de recabar los datos, ya sea directamente del interesado o de un tercero; 2) Al momento de tratar los datos; y 3) Al momento de utilizarlos, donde debe considerarse el conocimiento y consentimiento del titular.[154]

Para una mejor comprensión metodológica de este acápite, se dividirán los principios de protección de datos en atención a su aplicación nacional como también en doctrina internacional.

Así, en el plano nacional, los primeros principios que merecen consignarse, aplicables todos al tratamiento de datos que realice la Administración Pública en Chile y entre ellos a los establecimientos públicos de educación, son los siguientes: Principio de Licitud; Principio de Información; Principio de Veracidad de los datos; Principio de Finalidad de los datos; Principio de Seguridad de los datos; y Principio de Confidencialidad.

Por su parte la doctrina internacional ha dispuesto otros principios, adicionales a los ya expresados, entre los que se encuentran: Principio del

[154] INAI. 2014. Estudio sobre Protección de Datos a Nivel Internacional. Iniciación sobre los modelos de bases de datos, México. Pág. 26. [En línea] <http://inicio.ifai.org.mx/Estudios/prot_datos.pdf > [Consulta: 09 de agosto de 2016]

Consentimiento; Principio de Proporcionalidad; Principio de Responsabilidad; Principio de Categorías especiales de datos o datos especialmente protegidos; y, Principio de la Transparencia.

3.a) Principios aplicables a la legislación nacional de protección de datos personales

3.a.1) Principio de Licitud

Este principio informa que el tratamiento de datos personales sólo cabe en aquellos casos en que exista autorización legal o autorización por parte del titular, debiendo en este caso consistir en un consentimiento expreso. Conforme este principio los datos personales no se deberían recoger ni elaborar con procedimientos desleales o ilícitos; por tanto, tratamiento será lícito cuando todas las operaciones que se efectúen en relación con los datos personales cumplan con la normativa en la materia, y además sean leales.

Señala Osvaldo Gozaíni que “la licitud en la recolección de datos supone que las acciones emprendidas para la obtención de informaciones personales han dado cumplimiento a una pauta general de buena fe y lealtad hacia las personas interesadas”; consecuentemente, cualquier acción que implique

ocultación, engaño, apariencia, sigilo o cualquier otra maniobra elusiva de la verdad, constituirán un acto desleal en el tratamiento de datos personales.

En Chile la aplicación de este principio deriva de los artículos 2, 4 incisos 1 y 6, y 20 de la Ley Nº 19.628, al restringir el tratamiento de datos a las materias que sean de competencia de cada organismo, señalando expresamente que tal tratamiento debe ser *"con sujeción a las reglas precedentes",* añadiendo la norma citada que la Administración *"no necesitará el consentimiento del titular".*[155] En este punto, la opinión de Enrique Rajevic va en el sentido de que el artículo 20 constituye una autorización que permite a la Administración Pública el tratamiento de datos personales con relativa amplitud; sin embargo también reconoce que tal tratamiento debe ser con el resguardo de aplicar las demás reglas de la ley para salvaguardar los derechos de los particulares.

En atención a lo antes dicho resulta plausible entonces vincular a este principio con la regla de la finalidad – establecida en el artículo 9 de la Ley en comento -, que al restringir el uso de los datos que se recolecten sólo a los fines para los cuales fueron recogidos proscribe su entrega a terceros para finalidades distintas. En consecuencia, en el ámbito escolar los datos

[155] RAJEVIC, E., 2011. Protección de datos y transparencia en la Administración Pública Chilena. Inevitable y deseable ponderación. Expansiva UDP. En foco 162, ISSN 0717-9987, Chile. Pág 8. [En línea] <http://www.consejotransparencia.cl/consejo/site/artic/20130820/asocfile/20130820152206/protecci__n_de_datos_y_transparencia_en_la_administraci__n_p__blica_chilena.pdf> [Consulta: 11 de agosto de 2016]

personales, y sobre todo aquellos datos de carácter sensible deben ser tratados con el máximo rigor y protegerlos a todo evento; por ello todos los datos utilizados para actividades académicas, para elaboración de fichas clínicas de alumnos, para actualización de bases de datos de éstos, intercambios, servicio de transporte escolar o competencias deportivas, entre otras varias actividades, deben ser tratados por el responsable y por el encargado con lealtad, evitando los engaños en la recogida como asimismo en el propio tratamiento.

3.a.2) Principio de Información

Se trata de un principio general de protección de datos consistente en que toda persona tiene derecho a ser informada de determinados elementos cuando se le solicitan datos de carácter personal, a fin de que conozca quién, cómo y para qué serán éstos utilizados, y también ser informado de los derechos que la ley les reconoce.

En esta materia, las distintas leyes a nivel internacional han dispuesto que cuando se recaben datos de una persona para ser tratados, ya sea de forma automatizada o manual, se debe realizar de manera legal y además leal –principio de licitud -, lo que se traduce en que el interesado sea informado de modo expreso, preciso e inequívoco de la finalidad de la recogida, de los destinatarios de la información, y además ser advertido de la obligación o no de

contestar las preguntas que se le realizan y de cuáles pueden ser las consecuencias en el caso que se niegue a contestar o a proporcionar los datos.

En virtud de este principio, los responsables del tratamiento de datos personales se encuentran obligados a informar a los titulares de los mismos, las características principales del tratamiento al que será sometida su información personal, lo que se materializa a través del "aviso de privacidad"; por tanto, independientemente de que se requiera o no el consentimiento del titular para el tratamiento de sus datos personales, el responsable deberá siempre ponerlo a disposición.[156]

Específicamente en el sector educación, y a modo de ejemplo, debiera contemplarse la elaboración, por ejemplo, un aviso de privacidad para el tratamiento relativo al personal del responsable, es decir al responsable del establecimiento de educación pública y otro para sus clientes, ya sean proveedores u otras personas que eventualmente pudieran tener acceso a la información de establecimiento. El espíritu del principio en análisis supone que tantos los padres y apoderados, como los alumnos estén en disposición de poder controlar el tratamiento de sus datos personales, en el entendido que sólo a través del ejercicio de sus derechos podrá instar al responsable del

[156] En estos casos resulta pertinente aclarar que los responsables deben tener el número de avisos de privacidad que resulten necesarios de acuerdo con los tipos de tratamientos que realicen.

tratamiento, a que por ejemplo, cancele o modifique sus datos personales, todo lo cual será posible, a su vez, si éstos conocen en todo momento a quién debe dirigirse para tales efectos. [157]

En nuestro país, el principio de la información se plasma en la Ley Nº 19.628 a través del artículo 4, inciso 2º, que a su tenor señala: "…*La persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público.*", norma que obliga al responsable de la recolección y tratamiento a comunicar lo que sea pertinente al interesado con el fin de garantizar el conocimiento de la recolección, sus fines y destino, independientemente de cual sea el medio que se utilice para la recogida de los datos; constituyéndose como excepción el artículo 4 incisos 5 y 6: *"…No requiere autorización el tratamiento de datos personales que provengan o que se recolecten de fuentes accesibles al público, cuando sean de carácter económico, financiero, bancario o comercial, se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, o sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes y servicios.*

[157] INAI. Estudio sobre Protección de Datos a Nivel Internacional, Op. Cit. Pág. 54.

Tampoco requerirá de esta autorización el tratamiento de datos personales que realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficios general de aquellos."

Por su parte, y en este ámbito, en España la Ley Orgánica de Protección de Datos dispone en su artículo 5.1. que cuando los datos se soliciten directamente de su titular, el responsable del fichero (o su representante), cumplirá con su deber de informar al interesado, de manera previa y expresa, precisa e inequívoca: a) La existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de estos y de los destinatarios de la información; b) El carácter obligatorio o facultativo de sus respuestas a las preguntas que les sean planteadas; c) Las consecuencias de la obtención de los datos o de la negativa a suministrarlos; d) La posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; y e) La identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

En cuanto a la excepción de informar, el artículo 5.3. de la ley en comento establece que no será necesaria la información a que se refieren las letras b, c y d del apartado 1, si el contenido de ella se deduce claramente de la

naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.[158]

3.a.3) Principio de Veracidad

Al hablar del principio de veracidad nos referimos a la exigencia de que los datos personales respecto de los cuales se efectúa tratamiento sean de auténticos y correspondan a la realidad del titular de los mismos, es decir, que sean datos exactos, completos, pertinentes, actualizados y correctos. En este contexto, existen dos ámbitos de aplicación de este principio: por una parte el ámbito intrínseco del dato, y el otro, técnico – organizativo- El primero de ellos se traduce en la obligación del responsable del tratamiento de datos personales de verificar la exactitud y pertinencia de los datos registrados, como asimismo, cerciorarse de que siguen siendo lo más completos posibles a fin de evitar los errores por omisión y de que se actualicen periódicamente.

En Chile, el fundamento legal del principio en comento se encuentra en el artículo 6, inciso 2 de la Ley Nº 19.628, disponiendo a estos efectos que: *"Han de ser modificados cuando sean erróneos, inexactos, equívocos o incompletos",* lo que se traduce en que la información, o dato recabado o registrado en un

[158] CUIDA TUS DATOS. 2016. El derecho a la información en la Lopd. España. [En línea] <http://cuidatusdatos.com/obligacioneslopd/principioslopd/informacion/index.html> [Consulta: 05 de agosto de 2016]

sistema de datos personales, debe ser obtenida por medios legales, exacta, actualizada, y además apropiada para el fin para el que fue almacenada.

Para cumplir con este principio debe considerarse lo siguiente:

i) Si la información fue obtenida directamente del titular: Se presume que los datos son exactos, completos, correctos y actualizados pues emanan precisamente de quien es el dueño y titular de los mismos, hasta que éste no manifieste y acredite lo contrario; o bien, hasta que el responsable del tratamiento cuente con evidencia que lo contradiga y que haga necesaria su modificación.

ii) Datos obtenidos indirectamente: En tales casos, deben adoptarse las medidas pertinentes y razonables para que los datos personales contenidos en las bases de datos sean exactos, completos, pertinentes, actualizados y correctos.[159]

En este punto es esencial que al momento de la recogida de datos el responsable del centro educacional público verifique todos éstos, estableciendo su veracidad respecto de los alumnos, como por ejemplo datos relativos a su individualización, datos de contacto de sus padres, datos referidos a enfermedades y los respectivos cuidados especiales de alguno de ellos, tipo de

[159] INAI, 2014. Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, México. Pág. 59. [En línea] <http://inicio.ifai.org.mx/nuevo/Gu%C3%ADa%20obligaciones%20de%20la%20LFPDPPP.pdf > [Consulta: 08 de agosto de 2016]

alimentación, como también el eventual suministro de medicamentos en caso de ser necesario, entre otros. En cuanto a los apoderados, relevante también será fidelizar sus antecedentes identificatorios, su vinculación con el alumno, los datos de carácter social y económico que el establecimiento estime pertinente recabar y registrar, para de esta manera dar cuenta del cumplimiento al principio analizado.

Cabe señalar que este principio también se encuentra estrechamente vinculado con el principio de finalidad. Al respecto, Ana Herrán indica que el principio de veracidad de los datos se debe contemplar desde una doble perspectiva: la "calidad" del dato personal y la finalidad del tratamiento, de manera que los datos sean lícitos, en atención a que son puestos en relación con los fines legítimos que inspiran el tratamiento; sostiene que el dato será adecuado o pertinente cuando se encuentre directamente relacionado con la finalidad concreta, cuando sea necesario para el cumplimento de la misma, y por otro lado, también lo será cuando responda a la veracidad y exactitud e integridad de la información relativa a la persona.[160]

En este mismo orden de ideas, pero en el ámbito técnico – organizativo, debe introducirse el concepto de "calidad del dato", el que se traduce en que la finalidad con la que debe tratarse el dato exige su no permanencia en el

[160] HERRÁN, Op. Cit.

sistema de datos personales por un tiempo mayor al necesario para cumplir la finalidad para la que se obtuvo; por tanto, una vez concluido el plazo de conservación, y siempre que no exista disposición legal o reglamentaria que establezca lo contrario, el responsable debe proceder a la supresión de ellos, debiendo además establecer y documentar procedimientos para su conservación, bloqueo y supresión,[161] ello para que los procesos asociados al dato sean adecuados. B

Lo anterior refiere a la concreción del contenido del derecho, estableciéndose que el poder de disposición y control sobre los datos personales que tal derecho implica que se concreten jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular.

Por su parte ese derecho a consentir el tratamiento de datos personales, informático o no, requiere como dos complementos indispensables; por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos. En atención a lo anterior, el dato que trata el establecimiento de educación pública debe ser veraz, pero además, de calidad, debiendo los

[161] El plazo de conservación debe incluir un período de bloqueo, ya que los datos personales deben ser bloqueados antes de que sean eliminados o suprimidos.

datos seleccionados ser necesarios para lograr el objetivo general declarado de las operaciones de tratamiento, obligándose el responsable a limitar la obtención de datos estrictamente a la información que resulte directamente pertinente para la finalidad específica perseguida por el tratamiento. En este sentido, en la sociedad contemporánea debe hacerse una consideración adicional respecto de este principio, puesto que al utilizar tecnologías especiales para la mejora de la privacidad a veces es posible evitar el uso total de datos personales o bien, utilizarlos seudonimizados, lo que supone una solución respetuosa con el derecho a la privacidad.[162]

En resumen, el principio de veracidad – sumado a la calidad de los datos - propende el adecuado uso y tratamiento de los datos, para evitar con ello los tratamientos parciales, incompletos, fraccionados o que induzcan a error.

3.a.4) Principio de Finalidad

Al hablar del principio de finalidad nos referimos a uno de los principios más importantes e informadores del tratamiento de datos personales, puesto que se encuentra presente en las demás directrices atingentes al tema en análisis, y

[162] AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA. 2014. Manual de legislación europea en materia de la protección de datos. Consejo de Europa, Pág. 77. [En línea] <http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-es.pdf> [Consulta: 08 de agosto de 2016]

porque, además, es de aquellos principios que deben respetarse en las distintas fases del tratamiento.

Se entiende por finalidad del tratamiento el propósito, motivo o razón por el cual se tratan los datos personales, constituyéndose como obligación para el banco de datos especificar y justificar la finalidad de los mismos en el momento de su creación y ser objeto de una medida de publicidad o ponerse en conocimiento de la persona interesada a fin de que ulteriormente sea posible asegurarse que: a) Todos los datos personales reunidos y registrados sigan siendo pertinentes a la finalidad perseguida; b) Ninguno de esos datos personales sea utilizado o revelado sin el consentimiento de la persona interesada, con un propósito incompatible con el que se haya especificado; c) El período de conservación de los datos personales no exceda del necesario para alcanzar la finalidad con que se han registrado.[163]

Se persigue entonces que el tratamiento de datos personales sea informado al momento de la recogida de estos datos, debiendo perdurar la finalidad y estar presente en todas las etapas posteriores del tratamiento, salvo que exista consentimiento del titular de los datos.

[163] JERVIS, Op. Cit. Pág. 67.

Importante es precisar que la finalidad o finalidades del tratamiento de datos personales deberán ser determinadas, esto es, deberán especificar para qué objeto se tratarán los datos personales de manera clara, sin lugar a confusión y con suficiente objetividad. En ese sentido, el responsable del tratamiento de tales antecedentes personales deberá evitar que las finalidades que describa en el aviso de privacidad sean inexactas, ambiguas o vagas.[164]

En el ámbito educativo, el responsable deberá informar al alumno y a su apoderado al momento de registrarlo como tal y como parte de la institución, la finalidad determinada, explícita y legítima; informará por ejemplo el fin institucional perseguido, cómo utilizará todos los datos que el alumno entregue respecto de sí mismo y del grupo familiar, o quién utilizará tales datos, entre otros.

Básicamente lo que se pretende es que la institución pública de educación desarrolle una declaración de intenciones bien definida que sirva de referencia durante todo el proceso de diseño, la que le permitirá centrarse en los objetivos a la hora de tomar decisiones respecto de quienes se encuentren registrados en sus bases de datos.[165]

---

[164] Se debe evitar frases como "*de manera enunciativa más no limitativa*", "*entre otras finalidades*", "*otros fines análogos*", "*por ejemplo*" o "*entre otros".*

[165] MICROSOFT**.** 2016**.** Conceptos básicos del diseño de una base de datos. [En línea] **<** https://support.office.com/es-es/article/Conceptos-b%C3%A1sicos-del-dise%C3%B1o-de-una-

De acuerdo a la legislación mexicana, fructífera al igual que la española en materias de protección de datos, el Reglamento de la Ley Federal de Protección de Datos Personales en Poder de Particulares dispone que en este tópico existen dos tipos de finalidades: (i) aquéllas que dan origen y son necesarias para la relación jurídica entre el titular y el responsable, las cuales se identifican como primarias, y (ii) todas las demás que no cumplan con esta condición, las que se denominan secundarias o accesorias. Por ejemplo: Una persona – alumno - proporciona sus datos personales a un colegio para que le preste un servicio educativo y, a su vez, el colegio desea utilizar estos datos para invitarla a los eventos anuales que realiza. En este caso, la finalidad primaria está relacionada con la prestación del servicio educativo, en tanto que la finalidad secundaria o accesoria es la relacionada con la invitación a los eventos anuales. La ley mexicana distingue entre estas finalidades porque, de acuerdo con el artículo 42 del Reglamento citado,[166] el titular de los datos personales puede negar o revocar su consentimiento, así como oponerse al tratamiento de sus datos personales para las finalidades secundarias, sin que ello tenga como consecuencia la conclusión del tratamiento para las finalidades primarias. Por tanto, es indispensable que en el aviso de privacidad se identifique y distinga

---

base-de-datos-eb2159cf-1e30-401a-8084-bd4f9c9ca1f5#bmpurpose **>** [Consulta: 10 de agosto de 2016]

[166] Artículo 42. **"***El titular podrá negar o revocar su consentimiento, así como oponerse para el tratamiento de sus datos personales para las finalidades que sean distintas a aquéllas que son necesarias y den origen a la relación jurídica entre el responsable y el titular, sin que ello tenga como consecuencia la conclusión del tratamiento para estas últimas finalidades*"

entre las finalidades primarias y secundarias del tratamiento, indicando el mecanismo habilitado para que el titular, si así lo desea, pueda manifestar su negativa al tratamiento de sus datos personales para todas o algunas de las finalidades secundarias, mecanismo que debe estar a disposición de los titulares previo a que su información personal sea tratada para dichos fines.[167]

El artículo 9 de nuestra Ley de Protección de la Vida Privada consagra el principio en análisis, estableciendo en lo medular "*Los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público*…"; disponiendo además que los únicos casos en que su utilización puede tener una destinación distinta son aquellos en que su origen sea de una fuente accesible al público, esto es, cuando provengan de registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes.[168]

El precepto antes mencionado es amplio, debiendo entonces complementarse con lo dispuesto en el artículo 4 inciso quinto de la Ley en

[167] De acuerdo a la Ley de Protección de Datos mexicana, en aquellos casos en que el aviso de privacidad no se haga del conocimiento del titular de manera personal o directa, por ejemplo cuando se haga por envío postal, el aviso de privacidad debe indicar que el titular tiene un plazo de cinco días hábiles para que, de ser el caso, manifieste su negativa para el tratamiento de sus datos personales para las finalidades secundarias.

[168] Artículo 2, letra i) Ley N° 19.628.

comento, que establece la excepción, permitiéndose el tratamiento de datos personales que provengan de fuentes acceso público cuando éstos:

a. Sean de carácter económico, financiero, bancario o comercial;
b. Se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus título educativos, dirección o fecha de nacimiento; o
c. Sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.[169]

3.a.5) Principio de Seguridad

En términos generales, podemos sostener que la seguridad en materia de protección de datos debe procurar ser extremada al máximo con el objetivo de impedir el acceso a los sistemas de datos personales, en particular, y a los datos en general, limitando o restringiendo su acceso a personas no autorizadas o bien para evitar el desvío de la información, mal

[169] CENTRO DE ESTUDIOS EN DERECHO INFORMÁTICO. 2014. Las fuentes de acceso público en la protección de datos. Revista de Derecho y Tecnología, Vol. 3, Nro. 2, Universidad de Chile, ISSN 0719-2576, Chile. Pág. 12. [En línea] <http://www.rchdt.uchile.cl/index.php/RCHDT/article/view/33276> [Consulta: 11 de agosto de 2016]

intencionadamente o no, hacia sitios no previstos por la finalidad perseguida en su recogida.

Las medidas de seguridad tienen por objeto garantizar la confidencialidad y la integridad de los datos personales y evitar así su alteración, pérdida, transmisión y acceso no autorizado. La idea es preservar la confidencialidad e integridad de la información que es materia de tratamiento en los sistemas de información que contienen datos personales, debiendo adoptarse para ello las medidas de índole técnica y organizativa por quienes, por cualquier título, posean o traten datos personales. Lo antes dicho se fundamenta en que además la seguridad también debe ser tenida en cuenta para garantizar el tratamiento de datos dentro de los límites permitidos por la norma jurídica y con pleno respeto a los derechos del afectado y/o interesado.[170]

Según Osvaldo Gozaíni, este principio tiene dos facetas importantes: una, que atiende a la protección de los datos en particular; y la otra, al cuidado especial que se ha de tener con las personas que tratan la información y custodian la seguridad general del archivo. Para estos efectos será menester establecer y precisar un cierto grado de seguridad técnica que impida que la información se corrompa, destruya, o inutilice por casos fortuitos o “riesgos naturales”, como también, garantizar una seguridad lógica que impida que

[170] INAI. Estudio sobre Protección de Datos a Nivel Internacional, Op. Cit. Pág. 141.

terceros no autorizados accedan a la información personal que les permita por ejemplo, efectuar usos, modificaciones o divulgaciones indebidas de la misma, requiriéndose entonces comportamiento activo del responsable del banco de datos.[171]

De este modo y entendiendo que las medidas de seguridad son el control o grupo de controles de seguridad destinados a la protección de los datos personales, el responsable del banco de datos deberá tomar en cuenta los siguientes factores para así determinar el modo de implementación de tales controles: a) Riesgo inherente por tipo de dato; b) Consecuencias para los titulares por una vulneración; c) Sensibilidad de los datos; d) Desarrollo tecnológico.

Atendido lo expuesto y sin perjuicio del establecimiento expreso de este principio en el artículo 11 de la Ley Nº 19.628,[172] se hace necesario que el responsable del banco de datos garantice la seguridad de los datos personales a través de diversas medidas, las que en nuestro país se encuentran reglamentadas, respecto de los órganos públicos, por el Decreto Supremo N°

[171] JERVIS, Op. Cit. Pág. 65.

[172] Artículo 11 Ley N° 19.628, "*El responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños.*"

83/2004,[173] el que aprueba norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos. Se trata del cuerpo normativo que regula el ítem seguridad respecto de la protección de datos, sin embargo su médula está en normar el establecimiento de características mínimas obligatorias de seguridad y confidencialidad que deben cumplir los documentos electrónicos de los órganos de la Administración del Estado, y las demás cuya aplicación se recomienda para los mismos fines.

Las exigencias y recomendaciones contenidas en este Decreto tienen por finalidad garantizar estándares mínimos de seguridad en el uso, almacenamiento, acceso y distribución del documento electrónico; facilitar la relación electrónica entre los órganos de la Administración del Estado y entre éstos y la ciudadanía y el sector privado en general; y salvaguardar el uso del documento electrónico de manera segura, confiable y en pleno respeto a la normativa vigente sobre confidencialidad de la información intercambiada.

En virtud de lo expuesto, las instituciones educativas conscientes de la información personal y sensible que manejan, como también de los riesgos

[173] DECRETO N° 83. Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos. Fecha Publicación: 12 de enero de 2005. Ministerio Secretaria General de la Presidencia. [En línea] <https://www.leychile.cl/Navegar?idNorma=234598&idVersion=2005-01-12> [Consulta: 10 de agosto de 2016]

asociados a un mal tratamiento de datos por medidas de seguridad insuficientes, deberían aplicar algunas de las siguientes alternativas:

1. Capas de protección: Aplicación de *antimalware*[174] en todas las partes de la red**,** además de un firewall[175] en la puerta de enlace de la red escolar así como en todos los equipos individuales, ya sean propios, de concesiones, de estudiantes, de profesores y de empleados,[176] para así detectar y remediar *software* maliciosos en el sistema.

2. Implementación del principio del menor privilegio posible: El que se traduce en que sólo algunas personas tengan acceso con derechos de administrador a sus propias máquinas, debiendo usar solo su cuenta con privilegios mientras están realizando las tareas que la requieran.

3. Aplicar actualizaciones y revisiones a todo el *software:* Se debe considerar que no sólo los sistemas operativos y sus aplicaciones deben mantenerse actualizados, sino también aplicaciones auxiliares utilizadas por los navegadores. (Java, Flash, Adobe, etc.)

---

[174] El *antimalware* es un tipo de programa diseñado para prevenir, detectar y remediar *softwares* maliciosos en los dispositivos informáticos individuales y sistemas TI.

[175] *Firewall* o cortafuegos es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas; se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

[176] BURREL, B., WELIVESECURUTY (en español). 10 consejos para proteger la información de instituciones educativas. 2014. [En línea] **<**http://www.welivesecurity.com/la-es/2014/07/08/10-consejos-proteger-informacion-instituciones-educativas/> [Consulta: 11 de agosto de 2016]

4. Considerar que las contraseñas no son suficientes: En caso de proteger una cantidad importante de datos personales identificables, una sola contraseña puede no ser suficiente, por lo que debiese tomarse en cuenta la implementación de una doble autenticación, tal como control biométrico (huella digital), o tarjeta de claves digitales.

5. Cerciorarse que todos los profesores, alumnos y personal estén eligiendo buenas contraseñas: Se debe asegurar que todos sepan cómo hacerlas resistentes a ataques; esto es, que la contraseña sea única, fuerte, fácil de recordar para el usuario, pero difícil de adivinar para otros, la que debe ser larga, contener letras en minúsculas y mayúsculas, números y caracteres especiales.

6. Prohibir el compartir las credenciales: Ello en atención a que si los sucesos guardados en los registros no se pueden atribuir con certeza a la persona que los ejecutó, resultará muy difícil descubrir lo que realmente ocurrió cuando exista alguna irregularidad, razón por la que cada cierto tiempo debería ejecutarse un programa descifrador de contraseñas durante los inicios de sesión en la red.

7. Cifrar los datos en todas partes: Al tratarse de información valiosa para la entidad educadora, debe estar cifrada mientras no se usa directamente. En aquellos casos en que se necesite acceder a los datos o cuando se envían a través de la red, deben ser mediante conexión cifrada.

8. Realiza copias de seguridad: Las copias de seguridad de los datos y los sistemas constituyen la última y mejor línea de defensa ante los delincuentes destructivos. En el caso de considerar hacer la copia de seguridad en “la nube”, es conveniente realizarla como un complemento y no como un reemplazo de las copias de seguridad locales.

9. Capacitación de seguridad y toma de conciencia: A este respecto se recalca que tanto la entidad educativa (empleados – docentes), como alumnos deben estar al tanto de capacitaciones de seguridad, debiendo entonces explicarse cómo funcionan y por qué son necesarias las medidas de seguridad adoptadas.

10. Romper definitivamente con el pasado: En el caso de rotación de empleados y cuando los alumnos dejan la institución, es aconsejable asegurarse de modificar sus credenciales, lo que en muchos casos significa cerrar sus accesos a los sistemas de la escuela de forma inmediata, además de verificar anualmente cuentas de usuario autorizadas, y así eliminar permisos que ya no son apropiados.

De acuerdo a lo señalado en el artículo 2 del Decreto Supremo Nº 83 / 2004, sus disposiciones tendrán aplicación respecto de los documentos electrónicos que se generen, intercambien, transporten y almacenen en o entre los diferentes organismos de la Administración del Estado y en las relaciones de éstos con los particulares, cuando éstas tengan lugar utilizando técnicas y medios electrónicos, estableciendo que la seguridad del documento electrónico

en general se logra garantizando ciertos atributos esenciales, tales como: Confidencialidad; Integridad; Factibilidad de autenticación, y Disponibilidad, los que se obtienen y sostienen mediante: a) El desarrollo y documentación de políticas de seguridad de uso, almacenamiento, acceso y distribución del documento electrónico y de los sistemas informáticos utilizados en su procesamiento; b) El diseño y documentación los procesos y procedimientos para poner en práctica las políticas de seguridad; c) La implementación de procesos y procedimientos señalados precedentemente; d) El monitoreo del cumplimiento de los procedimientos y su revisión para evitar incidentes de seguridad; e) La concientización y capacitación a los usuarios para operar los sistemas informáticos de acuerdo a las exigencias establecidas; f) La definición de los roles y responsabilidad de las entidades e individuos involucrados en estos procesos.[177]

Por su parte, en este ítem la legislación chilena se ocupa de reglamentar el nivel básico y avanzado de seguridad del documento electrónico con el objetivo de garantizar su cuidado, seguridad e integridad. El nivel básico de seguridad, tiene por objeto garantizar condiciones mínimas de seguridad y confidencialidad en los documentos electrónicos que se generan, envían, reciben, procesan y almacenan entre los órganos de la Administración del Estado; además de facilitar la adopción de requerimientos de seguridad más estrictos por parte de

[177] Artículo 7, D.S. N° 83/2004.

aquellos organismos y en aquellos tópicos que se estimen necesarios, como asimismo facilitar el nivel avanzado de seguridad para el documento electrónico en aquellos organismos cuyo desarrollo institucional lo requiera, reglamentando para ello medidas tales como: Política de Seguridad; Seguridad Organizacional; Clasificación, control y etiquetado de bienes; Seguridad física y del ambiente; Seguridad del Personal; Gestión de las operaciones y las comunicaciones; Control de acceso; Desarrollo y mantenimiento de sistemas; y Gestión de continuidad del negocio.

En lo que respecta al nivel avanzado, el artículo 36 del documento en análisis señala que durante la segunda etapa de aplicación de esta norma, los órganos de la Administración del Estado deberán desarrollar las políticas, procedimientos, acciones y medidas tendientes a obtención del nivel avanzado de seguridad de los documentos electrónicos establecidos en el Título IV. Este nivel de seguridad para el documento electrónico exige el cumplimiento de las exigencias y condiciones reguladas en el Título IV para el nivel básico de seguridad, y las previstas en la Norma NCh2777,[178] (actualmente NCh 27002), que aplica tanto a documentos físicos como electrónicos, entendiéndose para estos efectos parte integrante del D.S. N° 83/2004.

[178] A este respecto señalar que el artículo 2° de la Resolución N° 1535 Exenta, Economía, publicada el 02.09.2009, anula y reemplaza la Norma NCh2777 por la Norma NCh-ISO 27002, que el artículo 1° de la mencionada Resolución, declara como Norma Oficial de la República de Chile, con su respectivo código y título de identificación como Tecnología de la información, Códigos de prácticas para la gestión de la seguridad de la información.

Precisamente estas normas son las que los órganos públicos en la materia - Ministerio de Educación, Consejo Nacional de Educación, la Agencia de la Calidad de Educación, y Superintendencia de Educación – refieren en general en sus documentos de seguridad; disponiendo a estos efectos básicamente que la recogida de los datos personales de usuarios – padres, apoderados, alumnos y comunidad en general – será en respeto a la finalidad establecida por la institución, que se adoptarán las medidas de seguridad necesarias para garantizar la confidencialidad de los datos recogidos, y que se hará especial prevención de que tanto el órgano público como los funcionarios que intervengan en cualquier fase del tratamiento de datos personales se verán obligados al secreto profesional respecto de los mismos y al deber de guardarlos; obligaciones que subsistirán aún después de finalizar sus relaciones con el Ministerio.

Agregan tales documentos que los datos que se entreguen serán administrados exclusivamente por los funcionarios de la institución, evitando usos indebidos, alteración o entrega a terceros y en caso de trabajar con entidades externas o empresas que administren base de datos, que se suscribirán acuerdos de confidencialidad que resguarden los datos personales. Reconocen además los derechos que la Ley N° 19.628 confieren a los titulares de los datos personales, como también se hacen cargo de las comunicaciones a terceros de los datos que traten, lo que en teoría permitiría colegir, en

principio, que existiría un cumplimiento de las normas sobre protección de datos personales tanto de alumnos como de la comunidad escolar en general.

A modo de complementación, cabe considerar en este acápite a la normativa mexicana, la que al respecto dispone en el artículo 61 del Reglamento de la LFPDPPP diversas acciones de seguridad a realizar por el responsable del tratamiento de datos. Entre ellos: i. Elaborar un inventario de datos personales y de los sistemas de tratamiento; ii. Determinar las funciones y obligaciones de las personas que traten datos personales; iii. Contar con un análisis de riesgos de datos personales consistentes en identificar peligros y estimar los riesgos a los datos personales; iv. Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva; v. Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales; vi. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha; vii. Llevar a cabo revisiones o auditorías; viii. Capacitar al personal que efectúe el tratamiento, y ix. Realizar un registro de los medios de almacenamiento de los datos personales; ello respecto de documentos electrónico como aquellos en formato físico.

Por otra parte, la ley española también se hace cargo de este ítem estableciendo que el Reglamento de Desarrollo de la Ley Orgánica 15/1999, se constituye en la actualidad como la normativa vigente en materia de medidas de seguridad aplicables a los tratamientos de datos de carácter personal, clasificando en su artículo 80 las medidas de seguridad aplicables a los ficheros o tratamientos de datos en tres niveles, debiendo adoptarse, en cada caso, el nivel correspondiente en función de la naturaleza de los datos a tratar.[179]

Así el artículo 81 del citado Reglamento dispone respecto de la aplicación de los niveles de seguridad lo siguiente: *"1. Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico. 2. Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal: a. Los relativos a la comisión de infracciones administrativas o penales. b. Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre. c. Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias. d. Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros. e. Aquéllos*

[179] Debe tenerse presente, además, que dichas medidas tienen un carácter acumulativo, de forma que las establecidas para cada nivel exigen incorporar las previstas para los niveles inferiores.

de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social. f. Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos. 3. Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal: a. Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual. b. Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas. c. Aquéllos que contengan datos derivados de actos de violencia de género."

Siguiendo en España, la Ley Orgánica de Educación (LOE) complementa con su Disposición Adicional Vigesimotercera a la Ley Orgánica de Protección de Datos y su normativa de desarrollo, fijando los datos personales que podrán recabar los centros docentes y estableciendo que la mera incorporación de un alumno a un centro supondrá el consentimiento para el tratamiento de sus datos personales y, en su caso, la autorización para la cesión de los datos procedentes del centro en que hubiera estado matriculado con anterioridad.

Dicha Disposición también hace referencia al deber de secreto por parte de los profesores y demás personal del centro de aquellos datos a los que tengan acceso con motivo del ejercicio de sus funciones, recomendándose que las cesiones de datos de un centro a otro se realicen de forma telemática asegurando una transferencia segura y efectiva. En atención a lo anterior, se ha de procurar por parte del centro educativo que solamente tengan acceso a los datos personales aquellas personas que, en cumplimiento de su función o cargo, estén autorizadas para ello.

Por último, mencionar la necesidad de tener redactado el correspondiente Documento de Seguridad que contenga las medidas de seguridad de índole técnico y organizativo que atañen al tratamiento de los datos personales en colegios, liceos (públicos y privados); de igual manera se deben adaptar los impresos de recogida de datos, formularios y contratos para que contengan las cláusulas informativas que exige la ley, pudiendo efectuar auditorías de cumplimiento (interna o externa)[180] por parte de un profesional experto en la

[180] Las que según Reglamento de Desarrollo de Ley Orgánica de Protección de Datos española, deberán ser, al menos, cada dos años. Art. 96.

materia, que determine si se está cumpliendo con los requisitos mínimos en este ámbito o bien indique las cuestiones que necesiten de adaptación.[181]

3.a.6) Principio de Confidencialidad

Preliminarmente señalar que la Directiva Europea 95/46 – aún vigente - en su artículo 16 establece este principio en los siguientes términos: "*las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento de datos personales, incluido este último, sólo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento o en virtud de un imperativo legal".* A este respecto mencionar que el citado precepto no establece la confidencialidad o secreto del tratamiento como una obligación de secreto profesional, sino como un deber de sujetarse en su actuación a las instrucciones o directrices del responsable del tratamiento, en cuanto los datos personales objeto del mismo. [182]

En virtud de lo antes mencionado, en este punto resulta importante distinguir entre conceptos que podrían – eventualmente - llevar a confusión: a) privacidad,

[181] MUÑOZ, J., 2009. Protección de datos personales en Centros Educativos públicos y privados. Privacy & Digital Business. España. [En línea] <http://www.joaquinmunoz.com/2009/05/12/proteccion-de-datos-personales-en-centros-educativos-publicos-y-privados/> [Consulta: 12 de agosto de 2016]

[182] JERVIS, Op. Cit. Pág.66.

b) confidencialidad o secreto y, c) seguridad referidos a los datos sometidos a tratamiento. En primer término, la privacidad hace referencia a que los datos son de una persona y que ésta tiene derecho a controlarlos y saber cómo se van a utilizar; la confidencialidad se refiere al mayor o menor secreto en que se van a guardar y tratar esos datos; y, por último, la seguridad hace referencia a las medidas de protección a tomar para la mejor defensa de la privacidad y grado de confidencialidad.[183]

Por tanto, es posible entender este principio como un "*deber*" que involucra la obligación de guardar secreto respecto de los datos personales que son tratados con el objetivo de evitar causar un daño a su titular, ya que de lo contrario, un tercero no autorizado podría tener acceso a una determinada información. Es por ello que este principio debe armonizarse con el principio de seguridad antes mencionado, puesto que cuando se tratan datos personales, el responsable tiene la obligación de adoptar medidas para evitar que quienes tengan acceso a éstos divulguen dicha información; inclusive ésta obligación debe hacerse cumplir una vez que finalice la relación contractual, laboral o de otra naturaleza entre el responsable del tratamiento y quien tenga acceso a los datos personales para el desarrollo de las tareas o funciones que se le hubieran encomendado, debiendo el responsable garantizar que este compromiso de

[183] DAVARA, M.A., 1998. La protección de datos en Europa. Principios, derechos y procedimiento. Madrid, Grupo Asnef Equifax, España. Pág. 24.

confidencialidad se cumpla, como se indicó, incluso una vez finalizada la relación con el titular de los datos personales.[184]

Concretamente en Chile, el artículo 7 de la Ley N° 19.628 dispone que "*Las personas que trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligadas a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con el banco de datos, obligación que no cesa por haber terminado sus actividades en ese campo"* con lo cual se verifica de manera práctica la aplicación del principio en comento.

En consecuencia, y para evitar accesos inadecuados a los datos personales, es que el responsable del registro debe cumplir con las obligaciones impuestas, estableciendo los ordenamientos jurídicos distintas recomendaciones que permiten la aplicación concreta del principio o deber a practicar, entre ellos quiénes y cómo accederán a los datos personales.

[184] INAI. 2014. Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, México. Pág. 67. [En línea] < http://inicio.inai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf > [Consulta: 25 de agosto de 2016]

En este punto la legislación mexicana recomienda:

a) Guardar confidencialidad de los datos personales, incluso después de finalizar la relación con el titular: a.1) Establecer procedimientos para evitar fuga de información o el acceso indebido a los datos personales; a.2) Capacitar al personal, tanto personal interno en régimen laboral, como externos y subcontratados, para que conozca sus obligaciones con relación al tratamiento de datos personales, como también de las consecuencias de su incumplimiento.[185]

b) Verificar que los encargados también guarden confidencialidad de los datos personales que tratan a nombre y por cuenta del responsable, aun después de concluida la relación con éste: b.1.) Incluir en los contratos u otros instrumentos jurídicos que celebre con terceros, cláusulas de confidencialidad y para que quienes tengan acceso a los datos personales en posesión del responsable cumplan con esta obligación de confidencialidad; b.2) Realizar verificaciones o supervisiones periódicas al trabajo realizado por los encargados, a fin de verificar que se cumplan con sus obligaciones en torno a la protección de los datos personales.[186]

[185] CUIDA TUS DATOS. s.a. España. El deber de secreto en la Lopd. [En línea] <http://cuidatusdatos.com/obligacioneslopd/principioslopd/secreto/index.html> [Consulta: 16 de agosto de 2016]

[186] INAI. Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Op. Cit. Pág. 68.

Cabe indicar que este principio toma aún más realce en materia educacional, puesto que la mayoría de los datos están referidos a menores de edad, antecedentes que revelan sus características propias, sus necesidades, padecimientos, tratamientos u otro que debe necesariamente ser protegidos tanto por el responsable, como por quienes traten directamente sus datos. Por tanto, es muy importante identificar y reconocer el perfil de los titulares de los datos personales, con el objeto de: i. Determinar previsiones particulares para menores de edad; ii. Definir el medio de difusión del aviso de privacidad que resulte pertinente, y, iii. Buscar la redacción adecuada del aviso de privacidad según la edad, nivel escolar, profesión, intereses, entre otros, del público objetivo.

Al respecto el Instituto Nacional de Transparencia, Acceso a Información y Protección de Datos – INAI-, en su "Guía práctica para generar el aviso de privacidad" propone algunos cuestionamientos que son de utilidad al momento de determinar si debe incorporar dicho elemento informativo en el aviso de privacidad: ¿Se tiene identificado que la organización trata datos personales de menores de edad?; ¿Existen medidas o acciones especiales implementadas para la protección de los menores?; ¿Se tiene implementado un mecanismo concreto para obtener el consentimiento de los padres o tutores de alumnos?; ¿El consentimiento de los padres o tutores para el tratamiento de menores incluye sólo los usos internos de la organización, y/o también refiere a

transferencias de datos que éstos realicen a terceros?; ¿A través de qué medios se verifica la autenticidad del consentimiento de los padres o tutores?; ¿Se proporciona información detallada sobre estas prácticas de privacidad de menores cuando se recaban los datos personales de éstos?; interrogantes que serán de utilidad para redactar el aviso de privacidad de acuerdo con el perfil del público objetivo y para reconocer el tratamiento de datos personales que requieran previsiones especiales, como el caso de menores de edad.[187]

3.b) Principios de doctrina internacional y su vínculo con la legislación chilena

3.b.1) Principio del Consentimiento

Como regla general se establece que el responsable del tratamiento de datos deberá contar con el consentimiento del titular para tales efectos; en estos casos la solicitud del consentimiento deberá ir siempre ligada a las finalidades concretas y específicas del tratamiento que se informen en el aviso de privacidad.[188]

---

[187] INAI. 2011. Guía práctica para generar el aviso de privacidad, México. Pág.18. [En línea] <http://inicio.ifai.org.mx/DocumentosdeInteres/privacidadguia.pdf> [Consulta: 16 de agosto de 2016]

[188] INAI. Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Op. Cit. Pág.14.

El titular de los datos debe prestar su consentimiento para que se pueda legítimamente efectuar tratamiento de su información personal, debiendo las excepciones a este principio ser establecidas por una norma legal. Se trata de un principio que recibe reconocimiento con mayor o menor fuerza en todas las legislaciones protectoras de datos, como asimismo, en las declaraciones de organismos internacionales sobre los principios rectores que deben estar presentes en materia de tratamiento de datos personales.

Específicamente, la autorización o consentimiento, por regla general, consiste en un acto expreso del titular de los datos por el cual consiente en que su información sea incorporada a un banco o registro de datos personales; aquel, antes de prestar el consentimiento debe ser informado a lo menos de la finalidad del tratamiento y el destino que tendrán éstos, puesto que la exigencia de este consentimiento se constituye en la base sobre la cual se estructura el derecho a la autodeterminación informativa, el que propende que el tratamiento de datos se efectúe a partir de una decisión libre y voluntaria de las personas.

A este respecto, Ana Herrán señala que “No hará falta insistir en la importancia que el derecho del consentimiento alcanza en la protección de datos personales, ya que a partir del reconocimiento de un derecho a consentir el tratamiento de los datos se estructura y organiza la autodeterminación

informativa o la facultad de los interesados de establecer y decidir sobre el tratamiento de la información que les concierne."[189]

En el plano del derecho comparado, especialmente, el europeo, se indican ciertas características que debe cumplir el consentimiento del titular de los datos, las cuales se pueden resumir en que éste debe ser: manifestado, libre, específico e informado.[190] Que el consentimiento sea manifestado quiere decir que se requiere que éste sea declarado, ya sea en forma tácita o expresa; en este caso nuestra ley no da cabida a interpretaciones sobre la posibilidad de una autorización tácita para efectuar tratamiento de datos personales, ya que exige que el titular consienta expresamente en ésta y que, además, tal manifestación conste por escrito.[191]

[189] HERRÁN, Op. Cit. Pág. 25.

[190] La Ley Orgánica de Protección de Datos española define el consentimiento en su artículo 3 letra h) estableciendo que: "Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el interesado consienta el tratamiento de los datos personales que le conciernen". Por su parte, La Ley 2.472 de la protección de las personas respecto al tratamiento de datos de carácter personal de Grecia (22.03.1997), en su artículo 2 dispone que el consentimiento es "toda indicación libremente prestada, explícita y específica, por la que el titular del dato expresamente y plenamente consiente; es decir, informado, consiente a que los datos relativos a él sean tratados". En Portugal, el artículo 3 letra h) de la Ley 67/98 de 26 de septiembre de 1998 sobre Protección de datos Personales define el consentimiento del titular de los datos como cualquier manifestación de voluntad, libre, específica e informada, por la cual el titular acepta que sus datos personales sean objeto de tratamiento. Al respecto señalar que todas estas legislaciones se inspiran en lo señalado en la Directiva Europea sobre la materia.

[191] JERVIS, Op. Cit. Pág. 85.

En cuanto al momento en que debe ser prestada la autorización en tanto manifestación de voluntad, la ley tampoco se pronuncia, pero es plausible concluir que debe ser anterior al tratamiento de datos que se pretende realizar, pues en caso contrario, no sería lícito al responsable del tratamiento actuar en atención a que no cuenta con la autorización inicial del titular de los datos.

El consentimiento libre refiere a la ausencia de vicios del consentimiento y aun cuando la Ley N°19.628 no señala, ello es posible colegirlo del cumplimiento de los requisitos que se presentan como generales en nuestro Código Civil.[192]

Con respecto a que el consentimiento sea específico, encontramos vinculados el principio del consentimiento con el principio de la finalidad; en este caso, aunque la Ley N° 19.628 no se refiere en forma expresa a este requisito del consentimiento, es posible observar que éste se encuentra recogido con mediana intensidad cuando se establece la obligación en el inciso segundo del artículo 4 para el que pretende efectuar tratamiento de datos de informar al titular de ellos el propósito del almacenamiento de sus datos y cuando el artículo 9 de la ley indica que tales datos se utilizarán sólo para los fines

[192] CÓDIGO CIVIL. Artículo 1445, Chile. *"Para que una persona se obligue a otra por un acto o declaración de voluntad es necesario: 1) que sea legalmente capaz; 2) que consienta en dicho acto o declaración y su consentimiento no adolezca de vicio; 3) que recaiga sobre un objeto lícito; 4) que tenga una causa lícita*."

respecto de los cuales se recolectaron, a excepción de aquellos que provengan o se hayan recolectado de fuentes accesibles al público; por ende, es posible colegir que la autorización debe ser específica con el objetivo de tener certeza respecto de las materias y datos respecto de los cuales se efectúa el tratamiento.

Por su parte, el consentimiento será informado cuando se cumpla con lo señalado en la legislación respectiva en cuanto a los contenidos que deben ser notificados al titular de los datos cuando éste presta su consentimiento. A este respecto, nuestra ley es menos exigente que las legislaciones existentes en otros países – por ejemplo la española -, ya que el inciso segundo de su artículo 4 sólo obliga a informar al titular de los datos respecto del propósito del almacenamiento de los datos personales y su posible comunicación al público, es decir, si los datos personales recogidos se darán a conocer a personas distintas del titular, sean determinadas o indeterminadas.

Excepciones:

El artículo 4 inciso primero de la Ley N° 19.628 indica el principio general existente en materia de protección de datos personales, tanto en nuestro país como en el ámbito internacional, esto es, que el tratamiento de éstos sólo

puede efectuarse cuando la misma u otras disposiciones legales de igual jerarquía lo autoricen[193] o el titular consienta expresamente en ello.

Para el caso chileno, tales excepciones a la autorización del titular de los datos que se indican en la propia Ley N°19.628 suelen ser agrupadas en cuatro y sin perjuicio de que han sido mencionadas anteriormente, se detalla lo siguiente:

i) Cuando los datos personales provienen o se recolectan de fuentes accesibles al público, y: a) Sean datos de carácter económico, financiero, bancario o comercial; b) Sean datos que se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento; o, c) Sean datos necesarios para

[193] Respecto a otras disposiciones legales que constituyan una excepción al consentimiento del titular de los datos, podemos encontrar disposiciones que en forma expresa autorizan el tratamiento de datos, como también normas que implican tácitamente una autorización para efectuar el tratamiento de los datos sin consentimiento de la persona a la cual éstos conciernen. Ejemplo del primer tipo de disposición encontramos la ley que crea el Consejo Nacional de la Cultura y las Artes y el Fondo Nacional de Desarrollo Cultural y las Artes, en la cual su artículo 3 Nº 12 señala como función del consejo: "*Desarrollar y operar un sistema nacional y regional de información cultural de carácter público. Para la operación del sistema nacional y regional de información cultural, a que hace referencia este numeral, el Consejo podrá crear un banco de datos personales, de aquellos señalados en la Ley 19.628*". Respecto a autorizaciones tácitas para efectuar tratamiento de datos, el Código del Trabajo establece en su artículo 10 las estipulaciones que debe contener el contrato de trabajo dentro de las cuales encontramos información personal del trabajador, como por ejemplo, su individualización, nacionalidad, fecha de nacimiento, ingreso. En este caso, al exigir la ley que el contrato de trabajo contenga datos personales del trabajador, el empleador se encuentra autorizado por una disposición legal a efectuar tratamiento de estos datos personales, sin necesidad, consecuentemente de una autorización expresa por parte del empleado, debiendo, en todo caso, el empleador cumplir con las normas que se indican en la Ley N° 19.628, respecto a la finalidad del tratamiento, seguridad, calidad de los datos, etc.

comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.

ii) Cuando se trate del tratamiento de datos personales que efectúen personas jurídicas privadas, siempre que se trate copulativamente: a) De datos personales para uso exclusivo de las personas jurídicas privadas, de sus asociados y de las entidades a que están afiliadas; b) El tratamiento se efectúe con fines estadísticos, de tarificación u otros de beneficio general de los mismos (artículo 4).

iii) En los casos de tratamiento de datos personales que efectúen organismos públicos respecto de materias de su competencia (artículo 20).

iv) Cuando el tratamiento de datos personales se efectúe para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares (artículo 10).[194]

Específicamente en el ámbito que nos ocupa, este principio tiene una aplicación especial, por cuanto no necesariamente el titular de los datos personales y/o sensibles será quien acceda a autorizar su tratamiento, puesto que hablamos en estos casos de menores de edad, cuyo consentimiento es prestado por sus padres o quien lo tenga a su cuidado personal de acuerdo a la legislación chilena.

[194] JERVIS, Op. Cit. Pág. 88.

En virtud de lo anterior, y al momento de la recogida de datos, serán los padres, apoderados u otro quien entregue su anuencia, expresa y a nombre del alumno menor de edad, para que los datos que se entreguen al establecimiento educacional sean incorporados a registro de base de datos y consecuentemente sean tratados. Sobre este punto, nos remitimos a lo señalado en el Capítulo II, acápite 2.b.3).

3.b.2) Principio de Proporcionalidad

Cuando nos referimos anteriormente al principio de finalidad, se indicó que sólo pueden recogerse datos de carácter personal y ser éstos tratados para el cumplimiento de una finalidad ya determinada, siempre y cuando los datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades legítimas para las cuales han sido obtenidos. De lo antes dicho surge entonces una vinculación del principio de finalidad con el principio de proporcionalidad, en atención que éste refiere que cuando el objetivo sea manipular datos de carácter personal para conseguir un fin, sólo podrán tratarse los datos estrictamente pertinentes para la consecución de dicho objetivo, regla que tiene pleno sentido desde la perspectiva del respeto al derecho fundamental a la autodeterminación informativa.[195] Así las cosas, y en atención

[195] ABERASTURI, U., 2011. Los Principios de la Protección de Datos aplicados en la Sanidad. Tesis presentada para la obtención del grado de Doctor en Derecho, Departamento de Derecho

al principio de finalidad, en caso que se manipularan más datos de los indispensables, el derecho a la autodeterminación informativa se vería innecesariamente afectado; por tanto, la exigencia es que en el ejercicio de la manipulación de datos con una finalidad determinada se cause el menor daño posible al citado derecho.

En todos aquellos casos en que exista una afección del aludido derecho, ésta necesariamente debe estar justificada, lo que viene aparejado del consentimiento de dicho titular de los datos para tratarlos o de la habilitación de una ley que reconoce que la manipulación de los datos de carácter personal es necesaria para la salvaguarda de un bien jurídico de mayor entidad; por tanto, para que tal justificación sea válida deberá existir coherencia entre los datos que se tratan y la finalidad que se persigue, naciendo entonces la obligación para el responsable del registro o banco de datos de no recabar ni tratar más datos de los estrictamente necesarios para alcanzar el fin que se propone.[196]

En el caso de España, la LOPD, dispone que sólo pueden recogerse y tratarse datos de carácter personal para el cumplimiento de una finalidad determinada, siempre y cuando esos datos sean adecuados, pertinentes y no

---

Administrativo, Constitucional y Filosofía del Derecho de la Universidad del País Vasco-Euskal Herriko Unibertsitatea, España. Pág. 196. [En línea] <https://addi.ehu.es/bitstream/10810/7664/17/ABERASTURI%20GORRI%C3%91O.pdf> [Consulta: 20 de agosto de 2016]

[196] REBOLLO, L., 2004. Derechos Fundamentales y la Protección de Datos. Madrid, Editorial Dykinson. España. Pág. 146.

excesivos en relación con el ámbito y las finalidades legítimas para las que se hayan recogido. Por su parte el Reglamento que desarrolla la Ley recoge una regulación prácticamente idéntica, con introducción de algún cambio, misma situación que se da con la Directiva Europea que reconoce la necesidad de que todo dato que vaya a ser manipulado sea adecuado, pertinente y no excesivo en relación a los objetivos perseguidos con el tratamiento.[197] Cabe sostener que el contenido del Convenio del Consejo de Europa es también muy similar en este aspecto.[198]

Mirado desde la perspectiva de la proporcionalidad, en el caso de utilización de cámaras de videovigilancia la situación es aún más compleja, en atención a que, entendiendo que la imagen es un dato personal, para efectos de captación y sobretodo registro es necesario contar con autorización legal o bien con el consentimiento del titular de ese dato. Así, en el contexto escolar, la instalación de éstas, con el objetivo de controlar determinadas conductas violentas, ha de ser una medida proporcional en relación con la infracción que se pretenda evitar y en ningún caso, debe suponer el medio inicial para llevar a cabo funciones de vigilancia, por lo que desde un punto de vista objetivo, la utilización de estos sistemas debe ser proporcional al fin perseguido, que en todo caso deberá ser

[197] Considerando 28 Directiva 95/46/CE: "*Considerando que todo tratamiento de datos personales debe (…) referirse, en particular, a datos adecuados, pertinentes y no excesivos en relación con los objetivos perseguidos (…*)"; Artículo 6.1 Directiva 95/46/CE: "*Los Estados miembros dispondrán que los datos sean (…) c) adecuados pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente*".

[198] Artículo 5, Convenio 108/1981 del Consejo de Europa.

legítimo, lo que siempre y cuando se limite estrictamente a esa finalidad. No obstante lo anterior, sería necesario atender las circunstancias particulares de cada centro educativo.[199]

En este sentido, si un establecimiento educativo determina la instalación de cámara de videovigilancia deberá comprobar que esta medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, y para ello será menester constatar que cumple los siguientes requisitos o condiciones: a) Que con medida adoptada es susceptible de conseguir el objetivo propuesto: seguridad para la comunidad escolar (juicio de idoneidad); b) Si además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia: Dotación de inspectores sea insuficiente para el resguardo de todos los alumnos (juicio de necesidad); y, finalmente, c) Si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto: obtención de antecedentes audiovisuales para determinar medidas de seguridad respecto de los alumnos (juicio de proporcionalidad en sentido estricto)".[200]

---

[199] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. 2016. Videovigilancia en los colegios, Informe del Gabinete Jurídico, España. Págs. 6 y 7. [En línea] <https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/videovigilancia/common/pdfs/2006-0262_Videovigilancia-en-los-colegios.pdf> [Consulta: 21 de agosto de 2016]

[200] PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN. 2012. España. Protec-Datos. Principio de Proporcionalidad. [En línea] <https://ofiseg.wordpress.com/tag/principio-de-proporcionalidad/> [Consulta: 21 de agosto de 2016]

La Ley N° 19.628 se refiere a este principio en el artículo 9 inciso 2°, el que dispone: "*En todo caso, la información debe ser exacta, actualizada y responder con veracidad a la situación real del titular de los datos*". Sin perjuicio de ello, se sostiene que este principio se acoge sólo parcialmente en nuestra legislación, en razón de que se omiten las demás exigencias, tales como que los datos personales sean adecuados, pertinentes y no excesivos. De esta manera un colegio podrá tener datos personales exactos, actualizados y veraces de los alumnos, pero ser al mismo tiempo, inadecuados, no pertinentes y excesivos, sin que exista norma ni principio que lo prohíba. El profesor Pedro Anguita Ramírez, sostiene que el artículo en comento parece impreciso al exigir dichas características a la "información" y no a los datos de carácter personal; señala que el artículo 6 de la ley en referencia también alude a este principio indicando que: *"Los datos personales deberán ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado.*

Han de ser modificados cuando sean erróneos, inexactos, equívocos o incompletos.

Se bloquearán los datos personales cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa y respecto de los cuales no corresponda la cancelación.

El responsable del banco de datos personales procederá a la eliminación, modificación o bloqueo de los datos, en su caso, sin necesidad de requerimiento del titular."

En este mismo sentido argumenta el profesor Anguita que, aun cuando forzosamente pueda señalarse que la “adecuación” queda comprendida en el inciso 1° del artículo antes referido, lo es en razón a que los demás incisos refuerzan las exigencias de “exactitud”, “actualización” y “veracidad” a que se refería el artículo 9. En consecuencia, y en su opinión, los requisitos o exigencias de pertinencia y adecuación de los datos personales no aparecen contemplados en la legislación chilena, motivo por el que sostiene que la legislación chilena no se ajustaría al principio de proporcionalidad.[201]

3.b.3) Principio de Responsabilidad

El término “responsabilidad”[202] proviene del mundo anglosajón donde es de uso general y donde se da una comprensión ampliamente compartida de su significado, aun cuando la definición exacta de «responsabilidad» resulta compleja en la práctica; se trata de un término que apunta sobre todo al modo en que se ejercen las competencias y al modo en que esto puede comprobarse.

[201] ANGUITA, P., 2007. La Protección de Datos Personales y el Derecho a la Vida Privada, Régimen Jurídico, Jurisprudencia y Derecho Comparado. Análisis de la Ley N° 19.628 sobre Protección de la Vida Privada (Protección de Datos de Carácter Personal), modificada por la Ley N° 19.812. Editorial Jurídica de Chile, Chile. Pág. 543 y ss.

[202] Accountability. En la mayoría de las demás lenguas europeas, debido sobre todo a diferencias en los sistemas de Derecho, el término «accountability» no es fácil de traducir, existiendo un gran riesgo de que el término se interprete diversamente llegándose con ello a una falta de armonización. Se han apuntado otras palabras para recoger el sentido de responsabilidad, como son «competencia reforzada», «garantía», «fiabilidad», fiabilidad» o, en español, «obligación de rendir cuentas», etc. Puede también sugerirse que la responsabilidad se refiere a la «aplicación de principios de protección de datos».

Competencia y responsabilidad son dos caras de la misma moneda y sendos elementos esenciales de la gobernanza, puesto que sólo cuando la responsabilidad funciona en la práctica puede desarrollarse la confianza suficiente.[203]

Este principio, conocido también como el principio de "rendición de cuentas", establece la obligación de los responsables de velar por el cumplimiento del resto de los principios, adoptar las medidas necesarias para su aplicación, y demostrar ante los titulares y la autoridad, que cumple con sus obligaciones en torno a la protección de los datos personales. Bajo este principio, los responsables del tratamiento están obligados a velar por la protección de los datos personales aun cuando los datos estén siendo tratados por encargados, y a adoptar las medidas suficientes para que los términos establecidos en el aviso de privacidad sean respetados por aquéllos con los que mantenga una relación jurídica.

Así las cosas, para cumplir con este principio, el responsable puede hacer uso de estándares, mejores prácticas internacionales, políticas corporativas, esquemas de autorregulación, y otros mecanismos que estime pertinentes. A modo de ejemplo, un titular de un centro educativo podría optar por desarrollar

[203] G29 (Grupo de Trabajo de Protección de Datos del artículo 29). 2010. Dictamen 3/2010 sobre el Principio de Responsabilidad, 00062/10/ES GT 173, Pág. 8 [En línea] <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_es.pdf> [Consulta: 25 de agosto de 2016]

una política corporativa en materia de protección de datos personales dirigida a quienes traten datos bajo su supervisión o por su cuenta, que incluya medidas y controles que sirvan para garantizar el cumplimiento de la normativa, debiendo el responsable tomar en cuenta que las medidas a adoptar, además de garantizar el debido tratamiento, deben privilegiar los intereses del titular – padres, apoderados y alumnos - y su expectativa razonable de privacidad.

Ahora bien, entre las medidas que el responsable puede adoptar para cumplir con el principio de responsabilidad se encuentran, al menos, las siguientes: a) Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización del responsable; b) Poner en práctica un programa de capacitación, actualización y concientización del personal sobre las obligaciones en materia de protección de datos personales; c) Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad; d) Destinar recursos para la instrumentación de los programas y políticas de privacidad; e) Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales; f) Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran; g) Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales; h) Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su

incumplimiento; i) Establecer medidas para el aseguramiento de los datos personales; j) Establecer medidas para la trazabilidad de los datos personales, esto es, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.[204]

En el caso de los establecimientos de educación, en ciertas ocasiones recurren a los servicios de terceras empresas o profesionales para cubrir determinadas necesidades del alumnado o de la propia institución; situación que toma especial trascendencia cuando, para la prestación del servicio solicitado, esa tercera empresa o profesional necesita tener acceso a los datos de carácter personal gestionados en el centro (por ejemplo, datos del alumnado). En este sentido, y siguiendo a la legislación española, el artículo 12.1 de la Ley Orgánica 15/1999 establece expresamente que *"no se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.";* ello puesto que ese tercero prestador del servicio es lo que la LOPD denomina *"encargado del tratamiento"*, esto es, *"la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o*

[204] INAI. Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Op. Cit. Pág. 64.

conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento".[205]

Entre los ejemplos más habituales de encargados del tratamiento en el ámbito educativo, y entre los que puede desprenderse responsabilidad, encontramos los siguientes:[206]

- La empresa prestadora del servicio de comedor escolar a la cual le puede ser proporcionado el listado de alumnos y alumnas apuntados al mismo, incluyendo, por ejemplo, posibles alergias a determinados alimentos.
- La empresa prestadora del servicio de transporte escolar a la cual se facilitan los datos de aquellos alumnos y alumnas que han solicitado el mismo.
- Las empresas encargadas del desarrollo e impartición de las actividades extraescolares del centro de enseñanza.
- Las empresas prestadoras de servicios de grabación de datos a las cuales se faciliten formularios donde puedan constar datos de carácter personal del alumnado del centro de enseñanza (solicitudes de vacante, matriculación, solicitudes de becas, etc.).

[205] Artículo 3. Letra g) Ley Orgánica de Protección de Datos, España.

[206] CONSERJERÍA DE EDUCACIÓN, Op. Cit. Pág. 80.

- Las empresas a las cuales se encomiende la recogida y posterior destrucción de toda la documentación en soporte papel inservible almacenada en el centro de enseñanza.
- El laboratorio fotográfico al cual se le facilitan el nombre y apellidos del alumnado del centro de enseñanza para confeccionar los diplomas académicos.[207]

Por su parte y en España, en aquellos supuestos en que la prestación de servicios no conlleve el tratamiento de datos de carácter personal, el contrato de prestación de servicios deberá, de conformidad con lo establecido en el artículo 83 párrafo segundo del Real Decreto 1720/2007, recoger expresamente la prohibición del personal ajeno de acceder a los datos personales de alumnos y la obligación de secreto respecto a los datos de éstos que hubiera podido conocer con motivo de la prestación del servicio. Este podría ser el caso de las empresas prestadoras de servicios de limpieza, cuya prestación no implica el tratamiento de datos de carácter personal, pero que, sin embargo, tienen acceso a las dependencias del centro de enseñanza donde se almacenan los datos de carácter personal del alumnado, personal docente, etc.[208]

[207] Cabe señalar que estos son sólo algunos ejemplos de un largo etcétera, pudiendo darse otros muchos supuestos de encargados de tratamiento en la casuística particular de cada centro de enseñanza.

[208] CONSERJERÍA DE EDUCACIÓN, Op. Cit. Pág. 80.

3.b.4) Principio de Categorías Especiales de datos o datos especialmente protegidos

En términos generales, los datos especialmente protegidos 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, a la vida sexual y los datos biométricos; así y desprendiéndolo de su propia denominación, los datos especialmente protegidos refieren a una categoría de datos que, por su especial naturaleza, requieren de un mayor grado o nivel de protección en miras a garantizar la privacidad de sus titulares.

Todas las normas internacionales sobre protección de datos hacen referencia, en mayor o menor medida a éstos, refiriéndose a ellos como “datos especialmente protegidos” o bien denominándolos “categorías especiales o particulares de datos”. Se ha señalado que preferiblemente es conveniente utilizar tal denominación al poseer el carácter de neutra, no refiriendo ninguna apreciación subjetiva, como si lo es el caso de nomenclaturas tales como “datos

sensibles", que en definitiva se aleja de la neutralidad y añade percepciones que también son preferibles evitar.[209]

En el caso de nuestro país, la norma habla directamente de Datos "sensibles". Específicamente en el artículo 2 letra g) dispone: *Para los efectos de esta ley se entenderá por*: *g) Datos Sensibles, aquellos datos personales que se refieren a características físicas o morales de las personas o hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.*

A este respecto cabe mencionar que tales antecedentes considerados de categoría especial, en ciertas legislaciones comparadas son establecidos como elementos taxativos de la norma, no enumeración meramente enunciativa, característica que no permite en consecuencia incluir en el concepto de datos sensibles a otros que no sean los específicamente mencionados por los referido textos legales.[210] En este caso, nuestro ordenamiento jurídico, en el estatuto relativo a datos personales en su artículo 2 utiliza la expresión "*tales como"* lo que aclara el carácter meramente enunciativo de los hechos, circunstancias o

[209] INAI. Estudio sobre Protección de Datos a Nivel Internacional, Op. Cit. Pág. 55.

[210] Caso argentino por ejemplo.

características físicas o morales que quedan amparados bajo el concepto de "datos sensibles", pudiendo en consecuencia establecerse otros no enumerados en ella que revistan esta misma característica y especificidad. [211]

La especial protección a la que se hace referencia, es posible concretarla en la práctica legal, en la necesidad de obtener, cuando sea necesario, el consentimiento del interesado o afectado en una determinada forma, pudiendo éste ser expreso y por escrito.[212]

A nivel internacional y como directrices relevantes en esta materia y específicamente en el principio en comento, se encuentra el Convenio 108[213] y la Directiva 95/46 CE, cuerpos normativos que sostienen y refieren a qué debe entenderse por "categoría especiales de datos". A saber, el artículo 6 del Convenio 108 señala que *"los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea*

[211] FERNÁNDEZ, H., s.a. Los datos sensibles en la Ley de Protección de Datos Personales, Argentina [En línea] < http://www.hfernandezdelpech.com.ar/PUBLICAtrabajosLosDatosSensEnLaLeyProteDatosPer.htm > [Consulta: 26 de agosto de 2016]

[212] INAI. Estudio sobre Protección de Datos a Nivel Internacional, Op. Cit. Pág. 128.

[213] CONVENIO DEL CONSEJO EUROPEO N° 108 PARA LA PROTECCIÓN DE LAS PERSONAS – también denominado Convenio de Estrasburgo - con respecto al Tratamiento Automatizado de Datos de Carácter Personal de 1981, cuyo objeto es conciliar el respeto de la vida privada y la libre circulación de la información a través de las fronteras.

garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a condenas penales."

Por su parte, la normativa contenida en el artículo 8 de la Directiva 95/46 CE dispone: "*1. Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad."*

Las normas aludidas contienen las previsiones sobre datos especialmente protegidos, lo que conduce a determinar que se trata de datos que poseen una naturaleza especial por su íntima conexión con la persona – titular – y, en su caso, mayor peligrosidad de su tratamiento ilícito, por lo que se hace necesario cubrirlas con una mayor protección.

Como hemos señalado anteriormente en lo relativo al tratamiento lícito de los datos sensibles, el Derecho del Consejo de Europa – CdE - remite al Derecho nacional para el establecimiento de la protección adecuada para el uso de los datos de categoría especial, mientras que el Derecho de la Unión Europea – UE -, en el artículo 8 de la Directiva de Protección de Datos, contiene un régimen pormenorizado del tratamiento de categorías de datos que revelen: el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas,

la pertenencia a sindicatos, así como datos relativos a la salud o a la sexualidad; en consecuencia y en principio, queda prohibido el tratamiento de éstos.[214] Sin embargo, existe una lista exhaustiva de excepciones a dicha prohibición, contemplada en el artículo 8, apartados 2 y 3 de la Directiva, entre las que se incluyen el consentimiento explícito del interesado, el interés vital del interesado, el interés legítimo de terceros y el interés público.

Contrariamente a lo que ocurre en el caso del tratamiento de datos no sensibles, no se considera que una relación contractual con el interesado constituya una base general para el tratamiento legítimo de datos sensibles; por tanto, si deben tratarse datos sensibles en el contexto de un contrato con el interesado, el uso de dichos datos exigirá la existencia de un consentimiento explícito autónomo del interesado, además del acuerdo de celebrar un contrato. Por su parte, una petición expresa del interesado de productos o servicios que revelarían necesariamente datos sensibles debería considerarse, sin embargo, equivalente a un consentimiento explícito.[215]

Rol relevante posee en estos casos el responsable del tratamiento, puesto que según el Derecho de la UE, al ser éste la persona que determine los fines y

[214] DIRECTIVA DE PROTECCIÓN DE DATOS, artículo 8, apartado 1.

[215] CONSEJO DE EUROPA. 2014. Manual de legislación europea en materia de la protección de datos. Agencia de los Derechos Fundamentales de la Unión Europea. [En línea] <http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-es.pdf PAGINA 94> [Consulta: 26 de agosto de 2016]

los medios del tratamiento de datos personales, sus decisiones establecerán el motivo y el modo en que los datos serán tratados. Según el Derecho del CdE, la definición de “responsable del tratamiento” menciona, además, que éste será quien decidirá qué categorías de datos personales deberán ser almacenadas.[216]

En nuestra órbita de análisis, ejemplos habituales de “datos especialmente protegidos” que pueden ser tratados en los centros de enseñanza son los siguientes:

- Los datos psicológicos contenidos en los informes psicopedagógicos, test de inteligencia y conducta, etc., confeccionados por los orientadores y orientadoras (datos referentes a la salud del alumnado).
- El dato del grado de discapacidad de determinados alumnos y alumnas con necesidades educativas especiales.
- Los datos sobre alergias a determinados alimentos de algunos alumnos y alumnas, para su conocimiento por parte del servicio de comedor escolar.
- Los datos referentes a determinados alumnos y alumnas que presenten problemas de salud que les imposibilite el ejercicio físico.
- El dato del origen racial de algunos alumnos y alumnas.

[216] CONVENIO Nº 108, artículo 2, letra d).

3.b.5) Principio de la Transparencia

Finalmente revisamos el principio de la Transparencia, el que refiere a un nuevo principio establecido en el actual Reglamento Europeo de Protección de Datos y que en definitiva comprende el Principio de la Información antes analizado, al que nos remitimos.

Sin perjuicio de lo anterior, cabe señalar que el Grupo de Trabajo 29 entiende por este, el deber de informar a los interesados acerca del objetivo del tratamiento y de la identidad del responsable del tratamiento en el tercer país y de todo elemento necesario para garantizar un trato leal, admitiéndose como las únicas excepciones las contenidas en el artículo 11, apartado 2, y 13 de la Directiva 95/46.[217]

[217] Artículo 11. Información cuando los datos no han sido recabados del propio interesado. Apartado 2: 2. Las disposiciones del apartado 1 no se aplicarán, en particular para el tratamiento con fines estadísticos o de investigación histórica o científica, cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados o el registro o la comunicación a un tercero estén expresamente prescritos por ley. En tales casos, los Estados miembros establecerán las garantías apropiadas.; Artículo 13.1. Los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones y los derechos previstos en el apartado 1 del artículo 6, en el artículo 10, en el apartado 1 del artículo 11, y en los artículos 12 y 21 cuando tal limitación constituya una medida necesaria para la salvaguardia de: a) la seguridad del Estado; b) la defensa; c) la seguridad pública; d) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas; e) un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales; f) tina función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e); g) la protección del interesado o de los derechos y libertades de otras personas.

En este ámbito de acción, y en nuestro país, la Ley N° 19.628 a través del artículo 4 inciso 2°, dispone que la información al titular de los datos recogidos es la premisa fundamental para su obtención y lógicamente para su tratamiento.

Sin perjuicio de lo anterior, el profesor Anguita sostiene que el principio en comento se acoge de manera muy limitada en nuestro ordenamiento jurídico, puesto que sólo se exige indicación del propósito, lo que debe ser entendido como sinónimo de finalidad. Refiere además que la frase “posible comunicación al público” es expresada en términos muy generales, lo que impediría su inclusión como una exigencia efectiva de la norma. Argumenta que la legislación chilena no obliga a señalar la identidad del responsable del tratamiento (nombre, dirección, teléfono), los destinatarios o las categorías de destinatarios, el carácter obligatorio o facultativo de las respuestas a las preguntas que se le formulen y sus consecuencias en caso de responder negativamente, la posibilidad de ejercer los derechos de acceso, rectificación y cancelación de los datos entre otras destacadas menciones. No obstante, en cuanto a la recolección de datos realizados para encuestas, sondeos de opinión y estudios de mercado, se debe entregar mayor información que en las demás recolecciones de datos personales al tener que comunicar a las personas, además del propósito para el cual se está solicitando la información, el carácter obligatorio o facultativo de las respuestas, según lo dispone el artículo 3 de la Ley N° 19.628. En consecuencia, y en opinión del profesor Anguita, es dable

concluir que nuestra legislación establece muy restringidamente el derecho a información en la recogida de datos, facultad esencial para garantizar adecuadamente este principio, por lo que en definitiva no se ajustaría a éste.[218]

En resumen y en término simples, lo esencial que propende el principio en comento es: a) Que el procesamiento sea transparente; b) Que se proporcione información sobre la identidad del controlador de datos; c) Que se indique el propósito del procesamiento; d) Que se informe a quién se le podrán revelar los datos personales; e) Que se señale cómo pueden ejercer sus derechos las personas; y f) Que se de a conocer cualquier otra información necesaria para el procesamiento justo de los datos personales.

En el caso español, y como se señaló al tratar el Principio de Información (acápite 3.a.2.) conforme a lo establecido en el artículo 5 LOPD, el alumno, la alumna o su padre, madre o representante legal, cuando así proceda, deben ser escrupulosamente informados con carácter previo a la recogida de sus datos, ya sea a través de los formularios de solicitud de vacante y matrícula, de la ficha que el profesorado utiliza para el control de sus alumnos y alumnas o a través de cualquier otro canal de recogida, de la finalidad para la que éstos se recogen, de los destinatarios de la información que faciliten, del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean

[218] ANGUITA, Op. Cit. Pág. 544.

planteadas, de las consecuencias de la obtención de los datos o de la negativa a suministrarlos, de la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición, así como de la identidad y dirección del responsable del tratamiento.[219]

En este ítem valga recordar la intrínseca relación entre los principios de consentimiento y de información, puesto que una de las características de todo consentimiento es que debe ser informado; por ende, en el ámbito escolar el consentimiento del alumno, sus padres y/o apoderados deberán ir, en todo caso, precedido de una declaración del titular del establecimiento educativo responsable del fichero en la que se informe de manera clara y precisa de la inclusión de sus datos en un fichero, de los usos que se prevé dar a los mismos, de los posibles destinatarios de los datos, entre otros, a fin de que aquel o aquella consienta o no a dar sus datos siendo plenamente consciente de a quién y para qué los está facilitando.

Finalmente, si la información se dirige a menores de edad, ésta debe expresarse en un lenguaje que sea fácilmente comprensible por ellos, según establece el artículo 13 Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

[219] CONSERJERÍA DE EDUCACIÓN, Op. Cit. Pág. 72.

3.c) Principios del Grupo de Trabajo 29:

Además de los principios ya enunciados, el GT29 en su Documento de Trabajo 1/08 sobre la Protección de Datos Personales de los Niños[220] dispone otra serie de principios orientados a este segmento de la población y específicamente en el ámbito escolar que resulta conveniente destacar. A saber:

3.c.1) Interés Superior del Niño: Referido a aquellas persona que no han alcanzado aún la madurez física y psicológica, razón por la que se refuerza la protección a su respecto, obligando a todas las entidades públicas y privadas que tomen decisiones relativas a los niños, como también los progenitores y los representantes de éstos, a respetar eficazmente este principio.

3.c.2) Protección y cuidado necesario para el bienestar de los niños: El principio del interés superior del niño exige una apreciación adecuada de la posición del niño, reconociéndole una inmadurez que lo hace vulnerable y que es menester compensar mediante la protección y cuidados apropiados que debe entregar la familia, la sociedad y el Estado; por ende, para alcanzar un nivel adecuado de cuidado para éstos, en ocasiones será necesario tratar sus datos personales de

[220] Directrices generales y en caso especial de los colegios. Adoptado el 18 de febrero de 2008.

manera exhaustiva involucrando a varios actores, lo que será además fundamental en área educación.

3.c.3) Derecho a la intimidad: La vida íntima del menor, de conformidad al artículo 16 de la Convención de Derechos del Niño, debe ser respetada inclusive por los representantes del mismo.

3.c.4) Representación: Se sostiene que los niños requieren representación jurídica para el ejercicio de la mayoría de sus derechos, lo que no se significa que la condición jurídica del representante tenga una prioridad absoluta o incondicional sobre el niño, pues deberán ser consultados a partir de cierta edad en aquellas cuestiones relativas a ellos. Cuando el tratamiento de datos del niño comience con el consentimiento de su representante y posteriormente aquél alcance la mayoría de edad, podrá revocar su consentimiento; para el caso que desee que continúe el tratamiento, deberá dar su consentimiento explícito cuando se le exija. Se recalca que los derechos del niño le pertenecen a él, mas no a su representante, quien solo se limita a ejercerlos.

3.c.5) Intimidad v/s Interés Superior del Niño: En este ámbito lo esencial es que se proteja la intimidad del niño del mejor modo posible, amparando sus derechos a la protección de datos personales. No obstante, en aquellos casos en que el interés superior del niño y su derecho a la intimidad parecieran estar

en conflicto, la protección de datos debe ceder al principio del interés superior; como por ejemplo que el Servicio de bienestar juvenil necesite información pertinente a abusos o negligencias respecto de menores.

3.c.6) Adaptación al grado de madurez del niño: Atendido a que el menor es una persona todavía en proceso de maduración, el ejercicio de sus derechos (que incluye la protección de datos), debe adaptarse a su nivel de desarrollo físico y psicológico; además los niños no sólo se encuentran en proceso de desarrollo, sino que tienen derecho a éste. En lo que respecta al consentimiento, la solución puede variar desde la mera consulta al menor, al consentimiento paralelo de niño y representante, hasta el consentimiento único del niño si ya es maduro.

3.c.7) Derecho a ser consultado: De manera gradual los niños van siendo capaces de contribuir a la toma de decisiones que les afectan y a medida que crecen se les debe consultar más regularmente sobre el ejercicio de sus derechos, incluyendo los relativos a la protección de datos. Esta obligación de consulta consiste en tener en cuenta (aunque no someterse necesariamente) las opiniones propias del menor, de las que pudiesen derivarse consecuencias a su respecto.[221]

[221] GRUPO DE TRABAJO 29. Op. Cit. Pág. 4 y ss.

CAPÍTULO CUARTO

ÓRGANOS DE CONTROL EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES EN MÉXICO, ESPAÑA Y CHILE

JURISPRUDENCIA EN MATERIA DE DATOS PERSONALES EN EL ÁMBITO DE LA EDUCACIÓN EN EL DERECHO LOCAL Y DERECHO COMPARADO

1) Contexto nacional y su mirada al derecho comparado

Quizás el tema de autoridad de control en el ámbito de la protección de datos sea el ítem que más provoca cuestionamientos y a la vez más nos aleja de países que han desarrollado de manera profusa la legislación en estas materias.

Se entiende que el control es aquella actividad desplegada con el afán de comprobar, inspeccionar o fiscalizar el desempeño propio o ajeno, constituyéndose un quehacer no sólo necesario, sino que indispensable en todo sistema jurídico organizado y que supone la concurrencia de dos elementos esenciales: el primero, la existencia de un determinado estándar normativo, de conocimiento del agente controlador y de quien es objeto de su actividad; y el

segundo, la formulación por parte del agente de control de un juicio de adecuación de la actividad de quien es controlado por tal patrón. Así, en mayor o menor extensión, las leyes de protección de datos conceden a las autoridades de control ciertas facultades cuyo ejercicio supone un previo requerimiento y resolución judicial. La intervención judicial prevista en las leyes sobre protección de datos no alcanza solamente al accionar del titular de datos que estima menoscabados sus derechos por el responsable del tratamiento, sino que también se extiende a las reclamaciones que este último formula contra las decisiones de la autoridad de control, así como a las acciones emprendidas por ésta en contra de aquél.[222]

Chile, como es de público conocimiento, no cuenta con un órgano garante que permita resguardar adecuada y correctamente el derecho que tenemos todos a la protección de aquellos datos respecto de los cuales somos titulares, lo que sin duda es aún un tema en discusión en nuestro país y que merece ser analizado en atención a lo delicado que resulta ser el tratamiento y un mal manejo de antecedentes de carácter personal y sensible de, por ejemplo, menores de edad que asisten a establecimientos educacionales, como también de todos los actores de la actividad educativa.

[222] CERDA, A., 2006. Mecanismos de Control en la Protección de Datos en Europa. *Ius et Praxis*, *12*(2), Chile. [En línea] < https://dx.doi.org/10.4067/S0718-00122006000200009> [Consulta: 21 de septiembre de 2016]

A este respecto, y aun cuando no existe órgano garante establecido legalmente, los esfuerzos para que esta situación se revierta se han venido suscitando desde hace algún tiempo; en la actualidad, varios proyectos de ley han sido ingresados al Congreso, y respecto de este ítem se postula básicamente a dos entidades para tales tareas. Por una parte, y en virtud del Proyecto de Ley que Regula la protección y el tratamiento de los datos personales suscrito por la Presidenta de la República en el mes de marzo de 2017,[223] se propone la creación de una Agencia de Protección de Datos Personales,[224] ante la cual los afectados podrán iniciar un procedimiento de tutela de sus derechos; y por la otra, el año 2016 el Consejo para la Transparencia – CPLT - a través de Oficio[225] dirigido al Senado de la República, manifestó su disposición en orden a constituirse en el futuro órgano garante en materia de protección de datos personales en Chile, indicando poseer y poner a disposición "*toda la experiencia institucional y el conocimiento adquirido en la*

[223] Mensaje Nº 001-365. Proyecto de Ley que Regula la protección y el tratamiento de los datos personales, que modifica las disposiciones de la ley N° 19.628 sobre Protección a la Vida Privada, promulgada en agosto de 1999; Iniciativa que forma parte de los compromisos asumidos en la Agenda de Probidad y Transparencia en los Negocios y en la Política, impulsada por el Gobierno de Michelle Bachelet.

[224] De acuerdo al proyecto de modificación de Ley Nº 19.628, la iniciativa contempla la creación de un nuevo servicio independiente y de carácter técnico, a cargo de velar por el cumplimiento de la normativa sobre tratamiento de datos personales y su protección, debiendo fiscalizar el cumplimiento de la ley. Asimismo, a esta entidad le corresponderá ejercer una labor de promoción y difusión de la protección de los datos personales y tendrá facultades para dictar instrucciones que permitan ir adaptando el marco regulatorio al desarrollo de las nuevas tecnologías.

[225] Oficio N° 2160 de 14 de marzo de 2016 emanado del Consejo para la Transparencia dirigido a Patricio Walker Prieto, Presidente del Senado que propone efectuar perfeccionamientos normativos a la Ley N° 19.628, sobre Protección de la Vida Privada.

implementación de un derecho fundamental, como lo es el derecho de acceso a la información, con la finalidad de constituirse en una posible solución ante la necesidad de contar con un órgano garante eficiente y eficaz."

Atendido lo anterior y a la indefinición de nuestro país respecto del órgano garante en la materia en análisis, es que la presente tesis dirigirá la mirada a España y a México, elección que no es antojadiza, pues se trata de dos países que vienen trabajando por lo menos hace más de 10 años en estos tópicos, que disponen por ley de una autoridad de control y que además han generado jurisprudencia que permite tenerlos como referentes al enfrentarnos a la disyuntiva de la entrega de antecedentes públicos que eventualmente puedan contener datos de carácter personal y/o sensible.

La particularidad que poseen estos órganos reside en que, en el caso de México su autoridad de control ostenta duplicidad de funciones, pues apuesta por la garantía del acceso a la información como también por la protección de los datos personales, erigiéndose el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales – INAI - como el órgano público encargado de resolver estos asuntos.

En España, la Agencia Española de Protección de Datos es el ente encargado de resguardar, tanto respecto de órganos públicos como de privados, los datos personales de los individuos.

En el caso de nuestro país, y aun cuando no existe norma expresa que le atribuya responsabilidad de ente garante de la protección de datos (además del artículo 33 letra m) de la Ley de Transparencia), no es posible dejar de considerar al Consejo para la Transparencia; órgano que a nivel nacional se erige como el ente de control del derecho de acceso a información pública y bajo ciertos lineamientos, también de la protección de datos de carácter personal, dictando a través de sus decisiones, - amén de las recomendaciones - la poca jurisprudencia que sobre la materia cuenta nuestro país.

2) Órganos garantes de la protección de datos personales en México, España y Chile

Atendida la importancia de la institucionalidad y las labores desarrolladas por estas entidades, pasamos a revisar la orgánica, ámbito de aplicación y funcionamiento de cada una de ellas, para luego revisar la jurisprudencia que respecto de datos personales de menores de edad han emitido:

2.a) México: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Durante el gobierno del Presidente Vicente Fox se da la iniciativa de ley que culminó con la promulgación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental – LFTAIPG -, que incluyó la creación del Instituto Federal de Acceso a la Información Pública –IFAI -. El año 2007 se reformó el artículo 6 de la Constitución Política de los Estados Unidos Mexicanos, estableciéndose el derecho a la información pública como un derecho fundamental en ese país; luego, el 27 de abril de 2010 el Congreso de la Unión aprobó la Ley Federal de Protección de Datos Personales en Posesión de los Particulares – LFPDPPP -, que amplió las facultades, atribuciones y responsabilidades del Instituto al considerársele como una autoridad nacional en la materia, y conjuntamente con ello, modificó su nombre al de Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales – INAI -.[226]

[226] WIKIPEDIA. 2016. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos. [En línea]< https://es.wikipedia.org/wiki/Instituto_Nacional_de_Transparencia,_Acceso_a_la_Informaci%C3%B3n_y_Protecci%C3%B3n_de_Datos_Personales> [Consulta: 14 de septiembre de 2016]

El INAI es un organismo constitucionalmente autónomo, descentralizado, no sectorizado, con personalidad jurídica y patrimonio propio,[227] cuya dirección y administración superior corresponden a un cuerpo colegiado - denominado Pleno - integrado por siete comisionados, quienes gozan de garantías de independencia y de plena autonomía constitucional para la conducción del Instituto y el ejercicio de sus atribuciones, expidiendo lineamientos y criterios en materia de clasificación de la información gubernamental y protección de datos personales, así como en la resolución de los recursos de revisión que las personas interpongan en contra de negativas de acceso a la información.[228]

La misión del INAI consiste básicamente en:

i) Garantizar el derecho de los ciudadanos a la información pública gubernamental y a la privacidad de sus datos personales; y,

ii) Promover en la sociedad y en el gobierno la cultura del acceso a la información, la rendición de cuentas y el derecho a la privacidad.[229]

[227] Artículo 33. Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Acceso a la información pública y protección de datos personales.

[228] INAI. México. 2016. [En línea] <http://inicio.inai.org.mx/SitePages/queEsPleno.aspx> [Consulta: 14 de septiembre de 2016]

[229] INAI. México. 2016. [En línea] < http://inicio.inai.org.mx/SitePages/misionViosionObjetivos.aspx> [Consulta: 14 de septiembre de 2016]

Por su parte, para el ejercicio de sus funciones cuenta con las siguientes facultades:

– *Atribuciones informativas:* Proporciona apoyo técnico a quienes soliciten el cumplimiento de las obligaciones establecidas en la ley; rinde cuenta al Congreso; desarrolla, fomenta y difunde análisis, estudios e investigaciones en materia de protección de datos personales en posesión de los particulares, brindando capacitación a los sujetos obligados.

– *Atribuciones normativas*: Interpreta la ley en el ámbito administrativo. Emite los criterios y recomendaciones, como también divulga estándares y mejores prácticas internacionales en materia de seguridad de la información.

– *Atribuciones de verificación*: Supervisa, vigila y verifica el cumplimiento de las disposiciones contenidas en la ley; elabora estudios de impacto sobre la privacidad previos a la puesta en práctica de una nueva modalidad de tratamiento de datos personales o a la realización de modificaciones sustanciales en tratamientos ya existentes.

– *Atribuciones resolutorias*: Conoce y resuelve los procedimientos de protección de derechos y de verificación, teniendo además funciones en materia de cooperación.

– *Atribuciones sancionadoras:* Impone sanciones pecuniarias previendo una serie de conductas consideradas como infracciones; tales sanciones van desde el apercibimiento hasta la imposición de multas máximas bajo un sistema de modulación de la penalidad, correspondiente a la gravedad de las conductas.

En contra las resoluciones del INAI las partes pueden promover el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa, lo que permite que los sujetos regulados cuenten con un medio de defensa idóneo y adecuado para la defensa de sus intereses y derechos en el orden administrativo.[230]

En México, hasta enero de 2017,[231] la legislación respecto de datos personales se dividía en dos frentes; por una parte la Ley Federal de Transparencia y Acceso a Información Pública Gubernamental, y por la otra la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. La primera, se constituye como el instrumento jurídico que reconoce por primera vez en México la protección de datos personales, limitando las bases de datos del sector público a nivel federal, estableciendo en

[230] VALENZUELA, D., 2016. Acceso a la información pública y protección de datos personales. ¿puede el Consejo para la Transparencia ser la autoridad de control en materia de protección de datos?, Revista de Derecho, Universidad Católica del Norte, Sección: Estudios, Año 23 - Nº 1, Chile. Págs. 66, 67 y 68. [En línea] < http://www.scielo.cl/scielo.php?pid=S0718-97532016000100003&script=sci_abstract> [Consulta: 14 de septiembre de 2016]

[231] Fecha de promulgación de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

su capítulo IV y en tan sólo 7 artículos (del art. 20 al art. 26) un marco general que regula la obtención, transmisión, uso y manejo de los datos personales en posesión de dependencias y entidades federales encargándose de disponer obligaciones para éstas, las que se traducen en: a) Obtener el consentimiento del titular para poder tratar sus datos personales; b) Informar a los particulares los propósitos para los que se recaban los datos; c) Adoptar las medidas técnicas necesarias para garantizar la seguridad de los datos personales que tratan y almacenan; d) Dar aplicación al principio de calidad, procurando que los datos sean exactos y actualizados; e) Reportar al INAI el listado actualizado de los sistemas de datos personales que posean a cualquier título.

A su turno, la LFTAIPG dispone los derechos de acceso y corrección de los datos personales que obren en poder de instituciones públicas, debiendo éstas responderlas dentro de plazo legal. Es de esta manera entonces que México se encarga de regular la protección de datos en la arista pública, estableciendo los procedimientos legales de rigor, que permiten el amparo efectivo de los derechos de los titulares.[232]

[232] MARTÍNEZ, E., 2011. El Derecho a la Protección de datos Personales en la Administración Pública Federal. Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco. México [En línea] < https://www.itei.org.mx/v3/micrositios/diplomado02/gdl/adjuntos/Sector_Publico_ITEI_18-19-nov-2011.pdf > [Consulta: 20 de enero de 2017]

En cuanto al ámbito privado, el reconocimiento al derecho de protección de datos personales tuvo un proceso paulatino. Desde el año 2000 se promovieron diversos proyectos legislativos sin que ninguno fructificara; luego, ya en el año 2007, el Congreso de la Unión aprueba una reforma al artículo 6º constitucional en el que establece la protección a los datos personales y la información relativa a la vida privada, así como el derecho de acceder y corregir los datos que obren en archivos públicos, pero no es sino hasta el año siguiente, con la aprobación de las reformas a los artículos 16 y 73 que se introduce al más alto nivel de la Constitución mexicana, el derecho de toda persona a la protección de su información. El artículo 16 constitucional reconoce y da contenido al derecho a la protección de datos personales, plasmándose en la reforma los derechos con los que cuentan los titulares: acceso, rectificación, cancelación y oposición (denominados por su acrónimo como derechos ARCO), haciendo referencia además a la existencia de principios a los que se debe sujetar todo tratamiento de datos personales, así como los supuestos en los que excepcionalmente dejarían de aplicarse dichos principios; reformas que sentaron las bases para la aprobación de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, entre cuyos beneficios destacan los siguientes:

- Se trata de un modelo híbrido que conjuga con un justo equilibrio los principios de protección de datos personales internacionalmente reconocidos y la libre flujo de la información personal para el crecimiento económico.

- Prevé mecanismos expeditos para el ejercicio de los derechos ARCO ante una autoridad independiente, además de sanciones para los casos en que deje de observarse la ley por parte de los sujetos regulados.

- Satisface los elementos básicos que garantizan la protección de los datos personales: principios, derechos, procedimientos (ante el responsable y ante la autoridad), definición de autoridades reguladora y garante; así como un catálogo de infracciones y de sanciones relacionadas con las mismas.

- Otorga una amplia protección a los llamados “datos sensibles”.

- Amplía la protección que actualmente gozan los datos personales en posesión del Gobierno en sus tres órdenes, al ámbito privado.

- Retoma elementos del Marco de Privacidad de APEC que lo hacen muy flexible al no imponer cargas excesivas e innecesarias de cumplimiento a los sujetos obligados, puesto que no se requiere un Registro de las bases de datos en posesión de los particulares.[233]

Recientemente en México se dicta la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados – LGPDPPSO [234] - , la que pasó a formar parte del paquete legislativo en que se sustenta el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos

[233] INAI. México. 2016. Cómo ejercer tu derecho a la protección de datos personales. [En línea] < http://inicio.ifai.org.mx/SitePages/Como-ejercer-tu-derecho-a-proteccion-de-datos.aspx?a=m1 > [Consulta: 15 de septiembre de 2016]

[234] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en vigor a contar del 27 de enero de 2017.

Personales, en conjunto con la Ley general de Transparencia y Acceso a la Información Pública y la Ley Federal de Transparencia y Acceso a la Información Pública, las que deberán ajustarse a las disposiciones previstas en la LFPDPPSO.[235] Se trata de una ley que tiene por objeto establecer los principios y procedimientos para garantizar el derecho a toda persona a la protección de sus datos personales cuando estos se encuentran en posesión de cualquier autoridad, entidad, órgano u organismos de los poderes ejecutivos, legislativo y judicial en el ámbito federal, estatal y municipal, así como órganos autónomos, partidos políticos, fideicomisos y fondos públicos. A su vez, introduce disposiciones sobre portabilidad de datos, regulando además la relación entre los sujetos obligados (en su carácter de responsables de los datos) y quienes intervienen como encargados, los medios para impugnar el procesamiento ilegal de datos personales y sanciones, como también un procedimiento de verificación que puede iniciarse de oficio por el INAI. Cabe mencionar que la entrada en vigor de la LGPDPPSO deroga todas las disposiciones en materia de protección de datos personales de carácter federal, estatal y municipal que contravengan lo previsto en ella. [236]

[235] Ajustes que de acuerdo a las previsiones de la Ley Mexicana, deberá realizarse en seis meses a partir de la entraga en vigor.

[236] CREEL; GARCÍA CUELLAR; AIZA Y ENRÍQUEZ., 2017. Ley General de Protección de Datos Personales. México [En línea] <http://www.creel.mx/noticias/general-law-for-the-protection-of-personal-data/> [Consulta: 30 de mayo de 2017]

Relevante en nuestro ámbito de análisis es que esta nueva ley establece que en el tratamiento de datos personales de menores de edad se deberá privilegiar el interés superior de la niña, el niño y adolescente, en términos de las disposiciones legales aplicables, [237] y en cuanto al consentimiento para la transmisión de datos personales por parte de menores y para el ejercicio de sus derechos ARCO, se estará a lo dispuesto en las reglas de representación previstas en la legislación civil que resulte aplicable.[238]

Finalmente señalar que la autoridad reguladora y facultada para ejercer las disposiciones de la ley en comento es el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.[239]

[237] ERP. 2017. Publican ley de protección de datos personales. Diario El Economista. 26 de enero de 2017. [En línea] < http://eleconomista.com.mx/sociedad/2017/01/26/publican-ley-proteccion-datos-personales > [Consulta: 30 de mayo de 2017]

[238] Artículo 20 inciso final y artículo 49 inciso 3 Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

[239] CREEL; GARCÍA CUELLAR; AIZA Y ENRÍQUEZ; Op. Cit.

2.a.1) Jurisprudencia relevante del INAI en protección de datos personales de menores en el ámbito educación [240]

i) Antecedentes en expediente

i.a) Expediente N° 1228/09**:**[241] Se solicitó a la Secretaría de Educación Pública el domicilio, número de teléfono de población estudiantil que tiene cada institución de nivel secundaria, pública y privada, ubicadas en el municipio de Ixtapaluca.

Del tenor de la resolución del órgano obligado es posible desprender que la Dirección General de Planeación y Programación de la citada Secretaría desarrolla un Sistema Nacional de Información, Estadística e Indicadores Educativos relacionados con la planeación, programación y evaluación del sistema educativo y establece la coordinación con el Instituto Nacional de Estadística, Geografía e Informática para la obtención y uso sistemático de la información estadística y censal, la que es difundida en el Sistema Nacional de Información Educativa. Revisada la normativa atingente a la materia, se deduce que los informantes del Sistema son las personas físicas y morales a quienes las Unidades les solicitan datos estadísticos, siendo éstas las áreas

[240] Atendido el ámbito competencial del INAI, cabe indicar que los casos expuestos pueden corresponder a establecimientos de educación privada.

[241] INAI. Resoluciones. [En línea] <http://consultas.ifai.org.mx/resoluciones/2009/1228.pdf> [Consulta: 15 de diciembre de 2016]

administrativas que cuentan con atribuciones para desarrollar actividades estadísticas y geográficas que permiten obtener información de interés nacional; a este respecto, los datos e informes que los particulares entreguen para fines estadísticos se manejan bajo observancia de los principios de confidencialidad y reserva y no pueden ser comunicados nominativa ni individualizadamente, ni tampoco utilizarse para otros fines que no sean estadísticos.

Señala el INAI que de acuerdo al contexto del expediente, es posible determinar que, en el marco de la Ley, los datos personales relativos a las personas físicas que los hagan identificables son información confidencial; sin embargo, lo solicitado fue el número de alumnos o estudiantes que conforman cada una de las instituciones, lo que se traduce en que no es procedente la clasificación de la información estadística de la población estudiantil, en atención a que su difusión no implicaría dar información nominativa o individualizada, ni tampoco se estaría divulgando información relativa a los informes que transgreda su anonimato. En virtud de lo expuesto, se revoca la clasificación de la información hecha valer por la Secretaría de Educación Pública, instruyéndose hacer entrega de la información al recurrente.

ii) Testimonios de alumnos

ii.a) Expediente N° 564/05:[242] La solicitud versó (entre otros) sobre copia certificada de distintos documentos relativos a queja por violencia sufrida por el requirente en Instituto Politécnico Nacional, especialmente testimonio de alumnos contenidos en el expediente.

El órgano requerido señala que no negó la información, sino que indicó al requirente que su presentación refería a información gubernamental y no a datos personales, le orienta a aplicar el procedimiento de acceso a información ante la misma entidad y que además los datos relativos a los testimonio de alumnos son clasificados como reservados, pues se vincula a una averiguación previa de la Procuraduría General de Justicia del Distrito Federal.

El INAI sostiene que resulta posible que los testimonio de los alumnos, generados u obtenidos por la entidad formen parte del expediente de una averiguación previa; sin embargo, tal argumento sólo puede ser invocado por la autoridad encargada de tal averiguación, esto es, por el Ministerio Público, quien posee el expediente. Además, los testimonios de los alumnos fueron obtenidos por la entidad reclamada en ejercicio de sus facultades, como parte de un acto de autoridad educativa; en consecuencia, se trata de actos de

[242] INAI. Resoluciones. [En línea] <http://consultas.ifai.org.mx/resoluciones/2005/564.pdf> [Consulta: 15 de diciembre de 2016]

autoridad distintos de los cuales además existen expedientes diferentes, sujetos ambos al procedimiento de acceso a información en sus respectivos niveles de gobierno (federal y local respectivamente). Señala además el Instituto que si una entidad determina que la difusión de la información puede causar serio perjuicio a las actividades de verificación de cumplimiento de las leyes, prevención o persecución de delitos, entre otros, deberá considerar el daño que causaría tal difusión; por tanto concluye que el procedimiento abierto por el Consejo Técnico Consultivo del establecimiento educacional ha acabado al emitir una resolución final en el ámbito de su competencia, agotando las formalidades del caso. Además, la información relativa a la toma de decisión originada por la queja del profesor contra los alumnos de la institución académica, una vez adoptada la decisión definitiva, constituye información pública en los términos de la ley y la figura de la averiguación previa no debe invocarse para reservar aquellos documentos que por su naturaleza son públicos, razón por la que se revoca la reserva de información referente a los testimonio de los alumnos.

No obstante lo anterior, los testimonios aludidos podrían contener datos personales relacionados con la intimidad de los declarantes – de entre ellos alumnos del establecimiento - o de terceros, por lo que al tratarse de acceso a la información, la entidad deberá elaborar una versión pública de los testimonios

citados que omita exclusivamente aquello que pudiera revelar la intimidad de las personas en los términos de la Ley.

iii) Solicitud de acceso y solicitud de cancelación de datos personales de menores

iii.a) Expediente PPD N° 0030/15:[243] La promovente en su carácter de representante legal del menor titular de los datos personales ejerció los derechos de acceso y cancelación ante la Universidad Iberoamericana, A.C. como entidad responsable. Ésta dio respuesta dentro del plazo de 20 días que dispone la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, señalándole que la información se encontraba a disposición, pero que la relativa a puntaje en examen de ingreso no se entregaba. Ante ello, la promovente recurre al INAI.

La argumentación del Instituto discurre en señalar que el titular, por su propio derecho o a través de su representante legal, podrá en cualquier momento, ejercer sus derechos de acceso, rectificación, cancelación u oposición respecto de los datos personales que le conciernen. Por su parte, el Código Civil Federal establece que al tratarse de datos personales de un menor debe estar

[243] INAI. Resoluciones. [En línea] < http://inicio.ifai.org.mx/pdf/resoluciones/2015/PPD%2030.pdf > [Consulta: 02 de febrero de 2017]

representado por quien ejerce la patria potestad – padres -, y en caso de impedimento de uno de ellos, será ejercida por el otro; en consecuencia, la promovente cumplió con los requisitos legales para ejercer el derecho de acceso y cancelación de los datos personales de su hijo menor.

Dentro de la sustanciación del procedimiento, el responsable señaló que los documentos solicitados por la promovente se encontraban a su disposición y que respecto al dato relativo a la calificación del menor, normalmente no se entregan, pero igualmente exhibió en versión digital el documento "Reporte de resultados generales de los sustentantes en orden alfabético" en donde obran los resultados obtenidos por el titular en su examen de admisión a la Prepa Ibero. Ante ello la promovente manifiesta su conformidad, por lo que el INAI arriba a la conclusión de sobreseer la solicitud de protección de datos, en atención a la manifestación de conformidad de la promovente con la respuesta otorgada por el responsable.

iii.b) Expediente PPD N° 0080/15:[244] El motivo de la reclamación deriva de la falta de respuesta del responsable – Instituto Tecnológico y de Estudios Superiores de Monterrey – a la solicitud de acceso y cancelación de los datos personales del titular presentada por su representante legal.

[244] INAI. Resoluciones. [En línea] < http://inicio.ifai.org.mx/pdf/resoluciones/2015/PPD%2080.pdf > [Consulta: 02 de febrero de 2017]

Dentro del procedimiento el responsable emitió respuesta a la solicitud en cuestión; sin embargo, la reclamante no quedó conforme, sosteniendo que no se le entregó la totalidad de los documentos en los que obran los datos personales del menor y de sus padres y que no estaba claro lo relacionado con el período de bloqueo.

El INAI fundamenta su decisión en que el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos y los artículos 1 y 38 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, tienen como objetivo la protección de los datos personales, que los titulares cuentan con los derechos ARCO para este amparo, y que dentro de las prerrogativas otorgadas se encuentran el derecho de acceso y cancelación. Para tales efectos, el titular, por su propio derecho o a través de su representante legal podrá, en cualquier momento, ejercer ante el responsable sus derechos ARCO a través del medio señalado en el aviso de privacidad respecto de los datos personales que le conciernen. Ante ello, el responsable tiene en todos los casos la obligación de dar una respuesta a las solicitudes, refiriéndose exclusivamente a los datos personales que específicamente se hayan indicado en la solicitud correspondiente, en el plazo de 20 días hábiles contados desde la recepción del requerimiento, y para el caso de no hacerlo, fundar su negativa en la ley, pudiendo el titular iniciar el procedimiento de protección de derechos.

Indica el INAI que si bien la ley en la materia no tiene disposiciones respecto de la protección de datos de niñas, niños y adolescentes, no es menos cierto que la Constitución y los Tratados Internacionales de Derechos Humanos, han fijado un modelo de protección integral, en el que se entiende que a aquellos les corresponden su reconocimiento al igual que para todos los seres humanos atendiendo a su especial condición; en consecuencia, los menores de edad gozan de la protección de cualquier injerencia sobre su vida personal y familiar, debiendo en el tratamiento de datos tener un especial cuidado respecto de sus datos personales. Por tanto, el Instituto tiene el imperativo legal de salvaguardar el derecho a la protección de los datos personales del menor hijo de la promovente, que en el caso concreto constituyen los datos personales entregados al responsable con motivo del proceso de admisión a la “Prepa Tec”.

Durante el procedimiento, el responsable puso a disposición de la promovente los documentos requeridos, incluyendo la solicitud de admisión, argumentando además respecto de las identificaciones de los padres que dicha información no está asociada al titular, siendo información ajena al procedimiento al implicar datos personales de terceros; sin embargo el responsable exhibió en formato PDF los documentos que obran en su poder.

Además el responsable manifestó que en su base de datos no obran datos personales adicionales a los ya exhibidos, por ende, en cuanto al derecho de cancelación, señaló que no existe disposición que lo obligue a conservar los datos personales por un período de tiempo específico, por lo que en plazo de 15 días procedería a la supresión definitiva de los datos personales asociados al titular; ello quedó certificado posteriormente ante Notario público, lo que implicó que el expediente abierto con motivo de la solicitud de ingreso del menor a la "Prepa Tec" fuera suprimido; por tanto, los derechos de acceso y cancelación de los datos personales del titular y de los padres han quedado sin materia, motivo por el que el INAI determina sobreseer la solicitud.

iv) Denuncia por incumplimiento de obligación de Aviso de Privacidad

iv.a) Expediente de Verificación N° 006/2016:[245] Se inicia el procedimiento por denuncia contra el Colegio Panamericano de Texcoco A.C. por incumplir su deber de poner a disposición su Aviso de Privacidad y hacer uso indebido de los datos personales de la titular y sus hijos menores de edad al realizar llamadas telefónicas a los números proporcionados por la denunciante sin su autorización ni consentimiento. La denunciante refirió que tiene una relación jurídica con el colegio en cuestión, pues éste es el responsable de la institución

[245] INAI. Resoluciones. [En línea] <http://inicio.ifai.org.mx/pdf/resoluciones/2016/03S%2002-0006.pdf > [Consulta: 02 de febrero de 2017]

educativa a la que asisten sus hijos y señala que no pusieron a su disposición el Aviso de Privacidad al momento de recabar sus datos personales, siendo estos utilizados para realizar llamadas telefónicas. El responsable reconoció haber realizado las llamadas y el número de teléfono corresponde a la institución reclamada.

En virtud de lo expuesto, el INAI acuerda iniciar el Procedimiento de Verificación en contra del Colegio Panamericano de Texcoco A.C., requiriendo a su representante legal para que informe respecto de los hechos plasmados en las denuncias, pero no se recibió respuesta.

Por su parte, notificado el responsable, no consta que haya efectuado descargos, confirmándose ante la autoridad que éste no proporcionó la información necesaria para acreditar el tratamiento de datos personales de la denunciante efectuado de conformidad a la ley en la materia, lo que permite concluir que incurrió en obstrucción a los actos de verificación del INAI.

A este respecto, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares establece que todo responsable tiene la obligación de contar con un Aviso de Privacidad – en formato físico y/o electrónico – para ponerlo a disposición de los titulares, cuyos elementos mínimos también son establecidos por ley; además el Instituto llevó a cabo una consulta en el sitio

web de la entidad responsable, constatándose que no existe ningún elemento referido al contenido respecto de la existencia de su Aviso de Privacidad, por lo que se considera que el responsable no cumple con la normativa vigente y su reglamento.

De lo anterior se colige que el responsable contraviene varios principios de la protección de datos: a) Principio de información, puesto que ha omitido la puesta a disposición del Aviso de Privacidad y no ha informado al titular de los datos las características principales del tratamiento al que serían o serán sometidos los datos; b) Principio del consentimiento, ya que no informó del Aviso de Privacidad respectivo cuando recolectó los datos personales, lo que no permite evidenciar que recabó el consentimiento de la titular para el manejo de datos personales y hace presumir que el responsable no obtuvo el consentimiento para tratar los datos de ésta ni de sus hijos, aunado a que éstos desconocían la finalidad para la que fueron recabados los mismos; c) Principio de responsabilidad, al no haber implementado estándares, mejores prácticas internacionales, políticas corporativas, esquemas de autorregulación o cualquier otro mecanismo que permita el manejo idóneo de los datos personales de la titular y de sus hijos, como tampoco existe documentación que permita presumir la existencia de medidas de seguridad, administrativas, técnicas y físicas para garantizar el debido tratamiento de los datos; y d) Principio de licitud, pues no

ha realizado el tratamiento de datos personales recabados con apego al cumplimiento de la norma sobre la materia.

En conclusión, en atención a que el responsable no presentó argumentos tendientes a acreditar que cumplió con los principios rectores de la protección de datos personales relativos al consentimiento, licitud, información y responsabilidad y a que obstruyó los actos de verificación del INAI, se determina ordenar iniciar procedimiento de imposición de sanciones, al no ajustar su actuación al ordenamiento jurídico.

2.b) España: Agencia Española de Protección de Datos

En Europa, específicamente en España nos encontramos con la Agencia Española de Protección de Datos – AEPD- , creada el año 1993,[246] la que se erige como el organismo público encargado de velar por el cumplimiento de la Ley Orgánica de Protección de Datos de Carácter Personal. Es un ente de derecho público, ostenta personalidad jurídica propia, goza de plena capacidad pública y privada, y actúa con independencia de las Administraciones Públicas

[246] En virtud del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos.

en el ejercicio de sus funciones, relacionándose con el Gobierno a través del Ministerio de Justicia.[247]

Además en el país ibérico existen agencias de protección de datos de carácter autonómico en Cataluña – Agencia Catalana de Protección de Datos – y en el país Vasco – Agencia Vasca de Protección de Datos -, las que tienen un ámbito de actuación limitado a los ficheros de titularidad pública declarados por las Administraciones autonómicas y locales de sus respectivas comunidades autónomas.[248] En cuanto a los ficheros privados de estas CCAA, éstos siguen siendo competencia de la Agencia Española de Protección de Datos.[249]

En cuanto a su estructura, la Agencia cuenta con un Director quien ostenta la representación de la misma durante sus cuatro años de mandato, considerándose sus actos como propios de ésta. Es independiente y es nombrado por Real Decreto de entre los miembros del Consejo Consultivo a propuesta del Ministerio de Justicia y de él dependerán jerárquicamente el

---

[247] ABANLEX. Información sobre la AEPD. s.a. España. [En línea] <https://www.abanlex.com/areas-de-practica/proteccion-de-datos/adecuacion-lopd/agencia-espanola-de-proteccion-de-datos/> [Consulta: 20 de septiembre de 2016]

[248] Como indicamos anteriormente, el 25 de septiembre de 2012 la Comunidad de Madrid anunció la supresión de la Agencia de Protección de Datos de la Comunidad de Madrid, que se materializó el 01 de enero de 2013, pasando sus funciones a ser asumidas íntegramente por la Agencia Española de Protección de Datos.

[249] WIKIPEDIA. 2016. Agencia Española de Protección de Datos. <https://es.wikipedia.org/wiki/Agencia_Espa%C3%B1ola_de_Protecci%C3%B3n_de_Datos> [Consulta: 20 de septiembre de 2016]

Registro General de Protección de Datos, la Inspección de Datos y la Secretaría de la Agencia. Sus actos (en representación de la Agencia) agotan la vía administrativa y contra ellos sólo puede interponerse recurso potestativo de reposición ante la propia AEPD o recurso contencioso – administrativo ante la Audiencia Nacional.[250] Existe también un Consejo Consultivo, que es el órgano colegiado de asesoramiento del Director, el que emite informe en todas las cuestiones que le solicite éste, formulando propuestas en materia de protección de datos.[251]

En cuanto al marco normativo de la AEPD, este viene regulado por su normativa específica, la que está compuesta por las siguientes disposiciones:[252] i) Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal (Título VI con rango de ley ordinaria).; ii) Real Decreto 1720/2007, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal.; iii) Real Decreto 428/1993 de 26 de marzo, por el que se aprueba el

[250] La Audiencia Nacional fue creada en virtud del Real Decreto Ley 1/1997 (BOE de 5 de enero de 1977). Es un órgano jurisdiccional único en España que tiene jurisdicción en todo el territorio nacional. Tiene su sede en Madrid, constituyendo un Tribunal centralizado y especializado para el conocimiento de determinadas materias que vienen atribuidas por Ley. En la materia específica que nos convoca, se ocupa de lo contencioso-administrativo, fiscalizando las resoluciones de la Administración del Estado.

[251] ABANLEX, Información sobre la AEPD, Op. Cit.

[252] Recordar que en mayo de 2018 comenzará a regir nuevo Reglamento Europeo de Protección de Datos.

Estatuto de la Agencia Española de Protección de Datos.; iv) Supletoriamente por la Ley 6/1997 de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado cuya Disposición Adicional 10ª establece el régimen jurídico de determinados entes públicos, entre los que se encuentra la Agencia Española de Protección de Datos.[253]

Las principales líneas de actuación de la Agencia Española de Protección de Datos, son las siguientes:

a) A instancia de reclamaciones privadas: Tratamiento de datos en Internet; Videovigilancia; Altas en contrataciones de servicios sin consentimiento; Inclusión en ficheros de información sobre solvencia patrimonial; Publicidad; Comunicación de datos a las autoridades de EEUU.

b) En cuanto a las Administraciones Públicas: Resoluciones que han tenido como objeto la calidad de los datos; deber de secreto; deber de información previo para acceder al correo corporativo de los trabajadores; listado sobre adscripciones políticas de funcionarios; análisis del aplicativo SIGO [254] que incorpora identificaciones realizadas por las agentes de la Guardia Civil.[255]

---

[253] AEPD. 2016. [En línea] < http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/conoce/marco-ides-idphp.php > [Consulta: 21 de septiembre de 2016]

[254] Sistema Integral de Gestión Operativa implementado por la Guardia Civil española, mediante el cual se introducen determinados datos de interés policial.

[255] CRUZ, J., 2014. 8 Claves para entender la Agencia Española de Protección de Datos. UNIR REVISTA, España. [En línea] < http://www.unir.net/derecho/revista/noticias/8-claves-para-

c) En relación a los responsables de ficheros y tratamiento de datos: Las funciones son emitir las autorizaciones previstas en la Ley; requerir medidas de corrección; ordenar, en caso de ilegalidad, el cese del tratamiento y la cancelación de los datos; recabar de los responsables de ficheros cuanta ayuda e información que estime necesaria para el desempeño de sus funciones; ejercer la potestad sancionatoria en los términos previstos por el Título VII de la Ley Orgánica de Protección de Datos; autorizar las transferencias internacionales de datos.

d) En lo que respecta a la elaboración de normas: Informar preceptivamente los proyectos de normas de desarrollo de la LOPD; informar los proyectos de normas que incidan en las materias propias de protección de datos; dictar instrucciones y recomendaciones precisas para adecuar los tratamientos automatizados a los principios de la LOPD; dictar recomendaciones de aplicación de disposiciones legales y reglamentarias en materia de seguridad de los datos y control de accesos a los ficheros.[256]

e) En relación a los afectados: Atender a sus peticiones y reclamaciones; facilitarles información de los derechos reconocidos en la Ley; promover campañas de difusión a través de los medios de comunicación.[257]

---

entender-la-agencia-espanola-de-proteccion-de-datos/549201452974/ > [Consulta: 20 de septiembre de 2016]

[256] ABANLEX, Información sobre la AEPD, Op. Cit.

[257] WIKIPEDIA, Op. Cit.

f) Otras funciones de la Agencia: Velar por la publicidad de los ficheros que incluyen datos de carácter personal, para lo que ofrece la posibilidad de consultar on line los ficheros inscritos, tanto públicos como privados;[258] cooperación con organismos internacionales y órganos de las Comunidades Europeas en materia de protección de datos; y representación de España en los foros internacionales en la materia.[259]

2.b.1) Jurisprudencia de protección de datos personales en área de educación emanada de la AEPD, respecto de menores de edad [260]

i) Relativo al Derecho de Acceso a datos personales de menores

i.a) Procedimiento N° TD/00881/2015:[261] Se solicita la información y cumplidos los requisitos para su ingreso, ésta no tuvo respuesta transcurrido el plazo establecido conforme a la Ley de Protección de Datos Personales Española por parte de la Asociación del Colegio Alemán de Madrid; no obstante

[258] Derecho de consulta al Registro General de Protección de Datos.

[259] ABANLEX, Información sobre la AEPD, Op. Cit.

[260] Atendido el ámbito competencial de la AEPD, cabe indicar que los casos expuestos pueden corresponder a establecimientos de educación privada.

[261] AEPD. Resolución Tutela de Derecho. [En línea] <http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2015/common/pdfs/TD-00881-2015_Resolucion-de-fecha-06-11-2015_Art-ii-culo-15-LOPD.pdf > [Consulta: 20 de diciembre de 2016]

posteriormente la entidad recurrida proporcionó acceso a la base de datos solicitados, su origen, finalidad y cesionarios.

A este respecto la AEPD sostiene que, conforme al apartado 45 de la Memoria Explicativa del Convenio 108 del Consejo de Europa, los datos relativos a la evaluación psicopedagógica de aptitudes, características de personalidad y preferencias profesionales de los alumnos son datos de salud, por lo que el titular de éstos - en este caso su representante - podrá acceder a los mismos. En cuanto al argumento esgrimido por la entidad recurrida, sobre que los datos que han quedado reflejados en sus informes de evaluación del menor y test realizados son anotaciones subjetivas y que los profesionales que la han elaborado han ejercido el derecho a retirar tales anotaciones, se señala que no cabe aceptar que se consideren las mismas anotaciones subjetivas en su totalidad; ello porque las referidas anotaciones son valoraciones personales sobre el menor, su entorno, actitud, comportamiento, reacciones no sustentadas objetivamente en datos clínicos, ya que la evaluación psicopedagógica se hace en base a datos, test o pruebas que permiten determinar el desarrollo psicológico, psicomotriz y estado emocional del solicitante de admisión, motivo por el que no puede tener la consideración de anotaciones subjetivas, menos aún las pruebas o test psicopedagógicos realizados. En consecuencia, la Agencia estima las reclamaciones formuladas, ordenando la remisión de la certificación en la que se facilite el acceso a los datos de salud del menor.

i.b) Procedimiento N° TD/00587/2015:[262] Se solicita la totalidad del expediente escolar de la hija menor al Concello de Monforte de Lemos y la Agencia dispone que la normativa vigente en materia de protección de datos establece el derecho de acceso del interesado a obtener información de sus propios datos personales, pero el acceso a documentos concretos no forma parte del contenido de este derecho de acceso, pretensión que queda fuera del ámbito competencial de la Agencia.

Por su parte, en cuanto al reclamante, señala que el progenitor no custodio que ostente la patria potestad sobre un menor y así lo acredite, tiene derecho a obtener copia de los datos relativos a su salud; además la evaluación psicotécnica de aptitudes, características de personalidad y preferencias profesionales de los alumnos se constituyen en datos psicológicos y se tratan como tal,[263] por ende, al ser datos de salud, el titular de los mismos o su representante podrán acceder a éstos conforme dispone la LOPD. No obstante, en el caso en particular, el reclamante no solicitó el acceso a la historia clínica de su hija menor (acceso regulado por la normativa vigente en materia de protección de datos) sino que solicitó copia de la totalidad de un expediente

[262] AEPD. Resolución Tutela de Derecho [En línea] <http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2015/common/pdfs/TD-00587-2015_Resolucion-de-fecha-11-09-2015_Art-ii-culo-15-LOPD.pdf> [Consulta: 15 de diciembre de 2016]

[263] INFORME JURÍDICO, Agencia Española de Protección de Datos 445/2009

administrativo, pretensión que queda al margen del ámbito competencial de la Agencia, razón por la que se desestima la reclamación formulada.

i.c) Procedimiento N° TD/00250/2010:[264] El reclamante ejerció derecho de acceso ante el Colegio de Educación Infantil y Primaria “Silos” y transcurrido el plazo no obtuvo respuesta legalmente exigible, pues el acceso se obtuvo fuera de tal plazo y de manera incompleta al no haberse informado el origen, finalidad y cesionarios de los datos conforme a la ley.

Señala el artículo 6 de la LOPD que el tratamiento de datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa; además no será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias, cuando se refiera a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento. Argumenta la resolución que, de acuerdo a lo establecido en la LOPD, el consentimiento se erige como una de las piedras angulares del principio de protección de datos personales; por tanto, el tratamiento de los datos del particular por parte de un tercero, en primera instancia, sólo se puede llevar a

[264] AEPD. Resolución Tutela de Derecho. [En línea] <http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2010/common/pdfs/TD-00250-2010_Resolucion-de-fecha-07-07-2010_Art-ii-culo-15-LOPD.pdf> [Consulta: 15 de diciembre de 2016]

cabo en el caso de que el titular de los mismos autorice dicho tratamiento, pudiendo esta autorización ser revocada en cualquier momento. En este contexto el artículo 6.1 de la LOPD vinculado a la disposición adicional vigésimo tercera de la Ley Orgánica 2/2006 de Educación,[265] Apartado 1 y 2, refiere a que los centros docentes podrán recabar los datos personales de su alumnado que sean necesarios para el ejercicio de la función educativa, señalando además el precepto que los padres o tutores y los propios alumnos deberán colaborar en la obtención de la información; que la incorporación de un alumno a un centro docente supondrá el consentimiento para el tratamiento de sus datos, y en su caso, para la cesión de datos procedentes del centro en el que hubiera estado escolarizado con anterioridad. Importante es destacar que la información a que refiere este articulado será la estrictamente necesaria para la función docente y orientadora, no pudiendo tratarse con fines diferentes del educativo sin consentimiento expreso. Adicionalmente la AEPD razona señalando que la comunicación de datos entre las Administraciones Públicas no supone la vulneración alguna de la normativa de protección de datos en la medida en que la conducta citada se encuentre prevista en la ley; en consecuencia, no se observa que se haya cometido vulneración alguna de la norma, estimándose procedente la reclamación. Se ordena se remita a la

[265] LEY ORGÁNICA 2/2006, de 3 de mayo, de Educación. España. Última actualización, publicada el 10/12/2013, en vigor a partir del 30/12/2013. [En línea] < https://www.boe.es/buscar/act.php?id=BOE-A-2006-7899 > [Consulta: 22 de diciembre de 2016]

reclamante certificación en la que se complete el acceso a sus datos y a los de su hija menor de edad, informando además el origen, finalidad y cesionarios.

i.d) Procedimiento N° TD/00080/2015:[266] El establecimiento educativo Los Soletes Proyectos Infantiles S.L. responde el requerimiento relativo a copia de informe de inspección educativa contenido en expediente de expulsión de hijas menores de edad, fotografías impresas sacadas en navidades, o en su defecto fichero digital de las fotografías, además de expediente completos de ellas, el origen de los mismos, los cesionarios y especificación de usos concretos y finalidades de su almacenamiento, y a su vez la Conserjería de Educación, Juventud y Deporte de la Comunidad Autónoma de Madrid deniega el acceso al indicar que este derecho queda limitado a los propios datos de carácter personal, no pudiendo ser considerada la información que recoge las declaraciones y datos de terceras personas incluida en el mencionado derecho, pues la entrega de tales antecedentes implicaría la revelación de los mismos a una persona distinta, hecho que no encontraría amparo en la LOPD.

En cuanto al centro educativo recurrido, éste accede a la entrega de los antecedentes, procediendo a atender el derecho de acceso en cuanto a los datos de base que obran en sus ficheros en relación al reclamante y sus hijas

[266] AEPD. Resolución Tutela de Derecho. [En línea] <http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2015/common/pdfs/TD-00080-2015_Resolucion-de-fecha-12-06-2015_Art-ii-culo-15-LOPD.pdf> [Consulta: 20 de diciembre de 2016]

menores de edad, su origen, finalidad y cesionarios. En consecuencia, la AEPD estima procedente la reclamación formulada, aun cuando determina que no procede la emisión de una nueva certificación por parte de la recurrida al haber atendido el derecho de acceso ejercido por la reclamante.

Por su parte, en cuanto a la Conserjería de Educación, Juventud y Deporte de la Comunidad Autónoma de Madrid, el razonamiento de la Agencia está dado en que el derecho de acceso previsto en la LOPD española consiste en obtener información de los datos personales de base registrados en los términos indicados en el artículo 29.3 del RDLOPD,[267] pero no ampara documentos concretos – como el referido informe – ya que dichos documentos pueden contener información relativa a terceras personas; argumenta además que el derecho de acceso es independiente del que otorgan a los afectados las leyes especiales y particularmente la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común – LRJPAC,[268] razón por la que la petición no puede considerarse como alguno de los derechos regulados por la LOPD, puesto que la normativa de protección de

[267] Artículo 29.3. Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos.: "*La información que se proporcione, cualquiera que sea el soporte en que fuere facilitada, se dará en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.*
Dicha información comprenderá todos los datos de base del afectado, los resultantes de cualquier elaboración o proceso informático, así como la información disponible sobre el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos."

[268] LEY 30/1992, de 26 de noviembre.

datos no ampara la solicitud de documentos concretos obrantes en un expediente concreto, pudiendo para ello utilizar los medios regulados por la LRJPAC. Es en atención a ello que la Agencia Española de Protección de Datos se considera incompetente para el análisis del caso, y desestima la acción en contra de la Consejería de Educación, Juventud y Deporte de la Comunidad Autónoma de Madrid.

ii) Relativo al Derecho de Cancelación al tratamiento de datos personales [269]

ii.a) Procedimiento N° TD/0116/2013:[270] Se solicita la cancelación de dato personal respecto de la Universidad Politécnica de Valencia – teléfono de contacto -, la que contesta señalando que está obligada por ley a tratar los datos para la prestación del servicio público de educación superior, y que en virtud de su competencia los tratan a través del Fichero del Alumnado de la Universidad, gestionándose en él todas sus actuaciones administrativas conducentes a verificar si los alumnos matriculados en sus centros cumplen con los requisitos necesarios para la permanencia en sus titulaciones y si finalmente éstos son merecedores de la obtención de los títulos oficiales que imparte.

[269] Jurisprudencia referida al área de Educación Superior.

[270] AEPD. Resolución Tutela de Derecho. [En línea] <http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2013/common/pdfs/TD-01116-2013_Resolucion-de-fecha-30-09-2013_Art-ii-culo-16-LOPD.pdf> [Consulta: 22 de diciembre de 2016]

Agrega la resolución que el artículo 33.1 del RDLOPD dispone que la cancelación no procederá cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado, las que justificaron el tratamiento de los datos. En consecuencia, estando basada la cancelación solicitada en la supresión del teléfono de contacto del reclamante, cabe mencionar que dichos datos son necesarios al existir una relación entre la entidad demandada y aquél, no procediendo dicha cancelación al ser el número de teléfono uno de los datos necesarios para contactar con el titular; además, el reclamante no aportó justificante alguno que haga necesaria la rectificación del dato referente al número de teléfono, motivo por el cual no resulta admisible la reclamación que origino el procedimiento de tutela de derechos.

ii.b) Expediente N° TD/00412/2014:[271] El reclamante señala que en la intranet de la Universidad Politécnica de Valencia existe un directorio de alumnos que incluye un buscador y que al introducir su DNI o un dato relativo a su nombre y apellidos aparece su nombre, apellido y correo de la Universidad, en circunstancias que no ha prestado consentimiento para figurar en dicho

[271] AEPD. Resolución Tutela de Derecho. [En línea] <http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2014/common/pdfs/TD-00412-2014_Resolucion-de-fecha-24-07-2014_Art-ii-culo-16-LOPD.pdf> [Consulta: 22 de diciembre de 2016]

directorio, por lo que solicita que la casa de estudios cancele los datos personales sobre los cuales se ejerce el derecho.

El establecimiento educativo argumenta que al momento de la recogida de los datos, en el impreso electrónico de matrícula que cumplimentó el reclamante, se informa a los alumnos que sus datos personales serán incorporados al fichero del alumnado para la gestión académica de los mismos y que a la aplicación intranet de la Universidad únicamente pueden acceder, previa identificación, a través de la utilización del nombre del usuario y contraseña los alumnos, estando restringido el acceso para otras personas; por tanto, ante una petición de cancelación de datos, ésta no procede por existir una obligación legal de mantenerlos para cumplir la relación que el reclamante tiene como alumno de la universidad. Refiere además la resolución que durante la tramitación del procedimiento y del examen de la documentación aportada, se deduce que la pretensión del reclamante es la revocación del consentimiento otorgado por el tratamiento de sus datos y no la cancelación de los mismos, por ello la Universidad ha manifestado que al tener conocimiento de dicha pretensión ha cursado de oficio la petición de exclusión en el buscador de intranet. En consecuencia, la Agencia desestima la reclamación de tutela de derechos al haberse denegado fundadamente la cancelación solicitada, y una vez determinada la pretensión del reclamante de exclusión de sus datos de

intranet, o revocación de su consentimiento, ha cursado dicha petición, por lo que se desestima su requerimiento.

iii) Relativo al Derecho de Oposición al tratamiento de datos personales

iii.a) Procedimiento N° TD/00168/2006:[272] El concurrente formula reclamación por la denegación del derecho de oposición al tratamiento de sus datos por parte del Instituto de Enseñanza Secundaria Pablo Serrano de Zaragoza.

La parte recurrida señaló que la presentación fue respondida el mismo día que ésta fue recepcionada, pidiéndosele que informara sobre qué datos de carácter personal que aparecen publicados en su sitio web infringen la normativa en la materia; sostiene que alguno de los datos personales utilizados han sido publicados en el Boletín Oficial del Estado y el resto lo ha sido considerando las obligaciones existentes para el instituto en la normativa que los regula.

Razona la Agencia indicando que la naturaleza del derecho de oposición y las condiciones refieren a un derecho personalísimo que se ejercerá

[272] AEPD. Resolución Tutela de Derecho. [En línea] <http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2006/common/pdfs/TD-00168-2006_Resolucion-de-fecha-06-09-2006_Art-ii-culo-17-LOPD.pdf> [Consulta: 15 de diciembre de 2016]

independientemente de los restantes derechos reconocidos por la LOPD a su titular, sin que quepa exigir contraprestación alguna por su ejercicio. En cuanto a los aspectos procedimentales relativos a la posibilidad de ser objeto de reclamación ante la Agencia y a la tramitación de las reclamaciones que se planteen, el artículo 18 de la LOPD establece una tutela de todos los derechos consistentes en que cualquier actuación contraria podrá ser objeto de reclamación ante la Agencia.

Agrega esta argumentación que la Directiva 95/46/CE en su artículo 14.b) establece que los Estados miembros reconocerán al interesado el derecho de oponerse, previa petición y sin gastos al tratamiento de los datos de carácter personal que le conciernan respecto de los cuales prevea un tratamiento destinado a la prospección. En este mismo sentido, el artículo 6.4 de la LOPD señala que en los casos en que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal y siempre que una ley no disponga lo contrario, este podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una situación concreta; en tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado, fundamentaciones de la reclamación que la AEPD estima conforme a derecho.

2.c) Chile: Consejo para la Transparencia

En el escenario local, la situación se presenta bastante distante a las realidades mexicanas y españolas por diversas razones. Al no existir un órgano de control encargado de velar por el cumplimiento de la Ley N° 19.628, amén de una legislación poco robusta, no existe aplicación práctica ni garantía de los derechos que ostentan los titulares de datos personales, lo que exige retomar la discusión con el objetivo de concretar la institucionalidad de un ente contralor de tratamiento de datos personales.[273]

El contexto no es auspicioso, pues la inexistencia de este órgano de control acarrea consecuencias que se vislumbran como nefastas para la protección de los datos personales, pues sin perjuicio que la ley en comento reconoce una serie de derechos a las personas naturales titulares de los datos, éstos deben ser ejercidos ante tribunales civiles en un procedimiento largo y costoso que en definitiva constituye una barrera para las personas comunes. A la fecha y luego de casi veinte años de vigencia de sus normas, no existe jurisprudencia civil de relevancia que arribe a conclusiones sancionatorias por el indebido tratamiento de datos personales.

[273] ÁLVAREZ, D., 2016. Acceso a la Información Pública y Protección de Datos Personales ¿Puede el Consejo para la Transparencia ser la autoridad de control en materia de Protección de Datos?. Revista de Derecho, Universidad Católica del Norte, Sección: Estudios, Año 23 N° 1, Chile. Pág. 52. [En línea] <https://dx.doi.org/10.4067/S0718-97532016000100003> [Consulta: 27 de septiembre de 2016]

La doctrina es unánime en señalar que nuestro país necesita una autoridad de control en materia de protección de datos, radicándose la discusión en determinar qué órgano será el encargado de esta misión. En la actualidad y como indicamos anteriormente, en virtud de diversos proyectos de ley enviados al Congreso, logra establecerse que uno de los focos de mayor atención se centra en la propuesta de una nueva institucionalidad, proponiéndose una Agencia Nacional de Protección de Datos dependiente del Ministerio de Hacienda por una parte; y por la otra al Consejo para la Transparencia – CPLT –.

En este sentido y para relevar el rol del Consejo en estas materias debemos señalar que de suma importancia resultó ser la reforma constitucional del año 2005 que confirió rango constitucional a los principios de transparencia en la Administración Pública y publicidad de los actos de Gobierno, los que se vieron notoriamente favorecidos. Por su parte, la Ley N° 20.285 sobre Acceso a Información Pública[274] el año 2008 logró generar el gran avance en materia de transparencia del sector público y acceso ciudadano, fijando un marco normativo institucional que contempla el establecimiento de nuevos mecanismos que permitan la obtención de información pública, la regulación detallada de las causales de reserva y la creación de un órgano autónomo legal

[274] Ley Nº 20.285 sobre Acceso a la Información Pública, Fecha de promulgación: 28 de agosto de 1999. Santiago, Chile. [En línea] < http://www.leychile.cl/Navegar?idNorma=276363 > [Consulta: 01 de octubre de 2016]

con facultades fiscalizadoras y sancionadores. La importancia de este órgano público en las materias en análisis está dado por el ejercicio de la atribución establecida en el artículo 33, letra m) de la Ley de Transparencia, que le entrega la misión de velar por el debido cumplimiento de la Ley N° 19.628 por parte de los órganos de la Administración del Estado y por la facultad de publicar recomendaciones específicas que debieran ser observadas como guía o parámetro respecto del tratamiento de datos personales que realizan los órganos públicos en el ejercicio de sus funciones.[275]

En cuanto a la naturaleza jurídica de este Consejo, se sostiene que al conocer de amparos por denegación de información está resolviendo "conflicto de derechos" (publicidad v/s reserva - protección de datos -) entre la Administración Pública y el solicitante, actuando de esta manera como un tercero frente a la controversia entre dos entidades: Administración y administrado. En consecuencia, al "decir el derecho", al determinar cuál es el derecho aplicable, si el acceso o la entrega de la información, o bien el secreto o reserva, estaría aplicando directamente jurisdicción. Según el profesor Alejandro Vergara Blanco, se trata de un órgano que ejerce jurisdicción contenciosa administrativa basado en un criterio funcional de jurisdicción, según lo dispone el artículo 19 N° 3 de la Constitución Política que no limita la garantía de un procedimiento racional y justo sólo a los tribunales que integran el Poder

[275] ÁLVAREZ, Op. Cit., Pág 61.

Judicial sino que al tribunal que señale la ley y que se halle establecido con anterioridad por ésta, para contraponerlos a las comisiones especiales y estando en la categoría constitucional del artículo 76 de la Carta Fundamental de los "demás tribunales", esto es, de los que no integran el Poder Judicial, quienes para hacer ejecutar sus resoluciones o practicar o hacer practicar los actos de introducción que decreten lo harán en la forma que la ley determine, de lo que es plausible colegir que esta corporación es funcionalmente un órgano administrativo que ejerce jurisdicción y que orgánicamente no forma parte del Poder Judicial.[276]

En este mismo sentido, la Corte de Apelaciones de Santiago, en la causa Rol N° 7938-10, caratulada "Servicio Civil con CPLT", dispuso en su considerando segundo que: "*Como cuestión previa, se ha sostenido por la reclamante que el CPLT carecería de competencia para elucubrar en torno al alcance del secreto que contemplan las disposiciones de la Ley 19.882. A este respecto baste señalar que, de acuerdo con el artículo 33 de la Ley de Transparencia, corresponde al Consejo Para la Transparencia resolver los reclamos por denegación de acceso a la información. Por consiguiente, está llamado a conocer y decidir sobre un conflicto de naturaleza contenciosa*

[276] HUEPE, F., 2010.. El Consejo para la Transparencia. Una aproximación a su funcionamiento. III Versión Seminarios, Probidad y Transparencia para la Administración, Chile Pág. 21. [En línea] <http://www.contraloria.cl/NewPortal2/portal2/ShowProperty/BEA%20Repository/Portal/Actualidad/Actividades/Seminarios/9-10122010/Zona_sur/El_Consejo_para_la_Transparencia.pd > [Consulta: 01 de diciembre de 2016]

administrativa…la labor de interpretación y de subsunción que es inherente a sus potencialidades decisoras. Al ser así, no puede aceptarse la pretendida incompetencia, para discurrir en torno al alcance del secreto previsto por la Ley 19.882, porque ello es consustancial a la misión del CPLT de definir si determinada información es o no susceptible de entregarse a quien la requiera;"[277]

En dichos de Jorge Jaraquemada Robledo,[278] mientras la Ley de Transparencia reconoce el carácter público de información que contiene datos personales, la Ley de Protección de la Vida Privada resguarda su confidencialidad; en consecuencia, ambas leyes tienen el mismo objeto de regulación: la información, radicando la diferencia en que la primera establece el régimen para acceder a la que obra en poder del Estado – dentro de la cual se incluyen datos personales dispersos – y considera un órgano garante; mientras que la segunda salvaguarda aquella que concierne a personas naturales identificadas o identificables y no considera una autoridad protectora de esos datos. Por tanto, cuando se trata de acceso a la información que involucra datos de personas distintas al solicitante y que se encuentran en poder de los servicios públicos, es usual que se presente una tensión entre

[277] INFORME DE JURISPRUDENCIA JUDICIAL, Corte Suprema, Corte de Apelaciones y Tribunal Constitucional sobre la Ley de Transparencia 2009- 2016. Unidad de Defensa Judicial, Dirección Jurídica CPLT / Febrero 2017. Pág 44. [Consulta: 15 de marzo de 2017]

[278] Actual consejero del Consejo para la Transparencia

ambas normas,[279] opinión compartida por Jessica Matus, quien señala que el principio de máxima divulgación contenido en la normativa sobre transparencia y el de finalidad en el caso de las normas sobre datos personales, ha tornado difícil el equilibrio entre ambos derechos, constituyendo una obligación de las instituciones la realización de un balance entre la transparencia y la lesión de derechos, antes de la divulgación de la información.[280]

A este respecto valga señalar que el Consejo para la Transparencia ha dado algunos pasos en estos tópicos, pero aun así sus atribuciones son limitadas y, por ende, no tan eficaces.

En este escenario, esta corporación se presenta como autónoma, de derecho público, con personalidad jurídica y patrimonio propio, cuya dirección y administración superior está radicada en un cuerpo colegiado con facultades resolutivas. Además, conforme al artículo 32 de la Ley de Transparencia, su objeto es promover la transparencia de la función pública, fiscalizar el cumplimiento de las normas sobre transparencia y publicidad de la información de los órganos de la Administración del Estado, y garantizar el derecho de acceso a la información. En cuanto a su labor de protección de datos

[279] JARAQUEMADA, J., 2015. La afectación de la vida privada como límite al acceso a la información. Revista Transparencia y Sociedad. Edición Nº 3, Chile. Págs. 34 y 35.

[280] MATUS, J., 2013. Derecho de acceso a la información pública y protección de datos personales. Revista Chilena de Derecho y Tecnología, Centro de Estudios Informáticos, Universidad de Chile, Vol. 2, Nº 1, Chile. Pág. 206.

personales, y como ya indicamos, es el artículo 33 letra m) del cuerpo legal citado el que contempla esta atribución, la que en definitiva se cumple mediante dos vías: a) Que las partes interpongan protección de un dato personal, debiendo el Consejo para la Transparencia pronunciarse al respecto, y b) Que el propio Consejo aplique directamente la legislación sobre protección de datos, ya sea porque esta aplicación influía en la decisión o porque se estimó que constituía una consideración adicional que debía tenerse en cuenta al momento de resolver el amparo en cuestión.[281]

En consecuencia, cabe sostener que aún cuando no existe un texto legal expreso que empodere al CPLT como el órgano garante en la protección de datos personales, no es menos cierto que su labor en este ámbito ha sido encomiable y ha sentado precedentes en algunos casos revisados, disponiendo, específicamente para el sector público, orientaciones de relevancia que son seguidas por éstos al momento de enfrentarse y decidir cuándo es necesario resguardar antecedentes personales requeridos a través del procedimiento de solicitudes de información pública.

En este escenario, el académico Daniel Álvarez sostiene – opinión compartida por quien suscribe esta tesis - que sería plausible otorgar al Consejo para la Transparencia las funciones y facultades necesarias para ungirlo como

[281] ÁLVAREZ, Op. Cit. Pág. 66.

la autoridad de control, promoción y protección de la vida privada tanto para los órganos públicos como también para el sector privado, lo que conllevaría lógicamente a la protección de la vida privada de niños, niñas y adolescentes en nuestro país.

Para avalar esta afirmación el mencionado autor esgrime en su artículo “Acceso a la información pública y protección de datos personales”, las razones más relevantes para atribuir al CPLT funciones de garante, como también las críticas que tal determinación ha merecido.

En cuanto a las razones para ostentar la calidad de autoridad de control, se encuentran: a) Mejor protección de ambos derechos (derecho de acceso – derecho a la protección de datos personales), ello por cuanto sabiendo que el tratamiento de datos personales en Chile ha sido desprolijo y deficiente, el CPLT ha demostrado ser eficiente en el cumplimiento de su misión – referida al acceso a información pública -; por ende, en caso de ser ampliadas esas atribuciones, podría colegirse que su actuación tendría las mismas características de eficiencia que ha demostrado a lo largo de estos años en su afán de promover la cultura de la transparencia; b) El mejor arbitraje de conflictos entre transparencia y protección de datos personales: Ello por cuanto esta corporación tiene ventajas comparativas respecto de cualquier otro órgano existente – o por crearse – de la Administración del Estado, puesto que sus

competencias atribuidas por ley, amén de la jurisprudencia dictada en orden a ponderar tanto el acceso a la información como la reserva – protección de datos –, lo instituyen como el órgano más idóneo en estas tareas; c) Mayor eficiencia en la administración de los recursos fiscales: Al tratarse de una única institución la que vela por los derechos de acceso a información pública y protección de datos personales, existe un ahorro de recursos al tener funciones que, en caso de estar en instituciones separadas, debieran duplicarse. Típicamente los procesos más estratégicos y transversales pueden tener economías de ámbito al estar radicados en una misma institución y por ende reducir el costo país de introducir la función de protección de datos;[282] ello se traduce en el aumento del presupuesto anual del CPLT que permita financiar las nuevas funciones a desempeñar y realizar las reformas orgánicas que se requieran para adaptar la institucionalidad que hoy dispone para enfrentar los nuevos desafíos.

En lo que respecta a las críticas a su eventual labor de órgano garante en materia de protección de datos, cabe mencionar el Informe del Centro de Sistemas Públicos de la Universidad de Chile, encargado por el CPLT – año 2010, aún atingente– que indica, a lo menos, tres aspectos críticos. A saber: a) Experiencia internacional: El mencionado informe señala e identifica a los

[282] CENTRO DE SISTEMAS PÚBLICOS DEL DEPARTAMENTO DE INGENIERÍA INDUSTRIAL. 2010. Informe "Diseño de un modelo organizacional del Consejo para la Transparencia en su nueva función de protección de datos", Facultad de Ciencias Físicas y Matemáticas de la Universidad de Chile, Chile. Pág. 111. [En línea] < https://datosprotegidos.org/informe-diseno-de-un-modelo-organizacional-del-consejo-para-la-transparencia-en-su-nueva-funcion-de-proteccion-de-datos/ > [Consulta: 15 de marzo de 2017]

países que tienen agencias exclusivas en materia de protección de datos, como España, identificando también a aquellos países que optaron por un modelo mixto, como es el caso de México. Ejemplo preponderante es la Agencia Española de Protección de Datos Personales,[283] conocida por su fuerza, capacidad y liderazgo, fuente de inspiración a otras legislaciones en la materia en análisis;[284] b) Las diferencias en los negocios: En este ítem se centra tal vez la crítica más importante, sobre todo en lo que respecta a principios, funciones, mercados y conflictos de intereses. De acuerdo a la opinión de Renato Jijena, no se consigna como idóneo tener en una misma institución las funciones de protección de datos y de acceso a la información, puesto que la experiencia internacional recogida demuestra que en su gran mayoría los temas los abordan agencias diversas en atención a que se trata de "negocios" muy distintos, considerando los principios involucrados, las funciones que deben desarrollarse, los sectores donde operan (no hay acceso en el sector privado) y que los conflictos de intereses se presentan también en ámbitos muy diversos;[285] c) Capacidad del CPLT para fallar contra sí mismo: Se parte de la base que esta crítica es posible realizarla a cualquier autoridad con facultades

[283] Obligación reiterada y reafirmada por el nuevo Reglamento Europeo de Protección de Datos.

[284] ÁLVAREZ, Op. Cit., Pág. 74.

[285] JIJENA, R., 2013. Tratamiento de datos personales en el Estado y acceso a la información pública. Revista Chilena de Derecho y Tecnología. Centro de Estudios en Derecho Informático, Universidad de Chile. Vol. 2, Nº 2, Chile. Pág. 93. [En línea] < http://www.revistas.uchile.cl/index.php/RCHDT/article/viewFile/30309/32096> [Consulta: 15 de marzo de 2017]

resolutivas, puesto que parte del control detentado sobre los órganos del Estado está constituido por la aplicación a los principios inherentes a un Estado de Derecho – por ejemplo, principio de legalidad, control y responsabilidad administrativa -, sumado el control jurisdiccional sobre sus actos u omisiones, conformando un sistema cautelar, al que se adscribe el CPLT.[286]

2.c.1) Jurisprudencia del CPLT en protección de datos personales de menores en el ámbito educacional

i) Información solicitada por padres y/o apoderados respecto de sus hijos o pupilos [287]

i.a) Requerimiento de informes psicológicos completos de evaluaciones realizadas a menores: A este respecto el CPLT razona indicando que, si bien el acceso al diagnóstico psicológico de una persona importa el acceso por parte de los reclamantes (padre o madre) a los datos personales sensibles de un tercero (hijo menor de edad), en tales casos no resulta aplicable el régimen de resguardo de dichos datos reglado por el artículo 10 de la Ley Nº 19.628, toda vez que los reclamantes han acreditado la representación legal del titular de

[286] ÁLVAREZ, Op. Cit., Pág. 75.

[287] Roles: C632-12; C967-12; C1562-12; C544-13; C832-13; C1202-13; C1592-13; C2074-13; C2738-14; C230-15 y C2839-15; decisiones que se encuentran a disposición del público en el sitio web institucional del Consejo para la Transparencia www.cplt.cl, a través de la siguiente ruta: Portada / Banner "Seguimiento de Casos". Vínculo directo de ingreso: http://www.consejotransparencia.cl/consejo/stat/search/search_results.html?filtro_busqueda=seguimiento

dichos datos; además, en algunos casos, habiendo sido oído el titular, éste accedió a la entrega. Esto último refiere a gestiones propias realizadas por el CPLT a fin de atender la opinión que el menor pudiera manifestar respecto del requerimiento, de conformidad a la Convención sobre los Derechos del Niño –CDN-, quienes son considerados sujetos de derechos distintos a los padres, debiendo ser oídos como sujetos de opiniones propias cuando estén en condiciones de formarse un juicio.[288]

El CPLT sostiene que no puede impedirse a un padre conocer los antecedentes relativos al estado de salud de sus hijos en razón de no ejercer la patria potestad, y en consecuencia, no ostentar su representación legal; ello atendido a que la CDN impone a ambos padres un deber de crianza, que va más allá del cuidado personal y que no sólo corresponde a quien tenga la patria potestad, lo que supone un conocimiento de las condiciones en que se encuentra el menor, particularmente en materia de salud.[289] Por su parte, el principio del interés superior del niño, consagrado en la CDN y en los artículos 222 y 242 de nuestro Código Civil, puede desarrollarse en mayor medida si ambos padres están al tanto de los estados de salud de sus hijos, entendiendo

[288] CPLT. Amparo C632-12. Enlace directo: [En línea] <http://extranet.consejotransparencia.cl/Web_SCW/Archivos/C632-12/C632-12_Decisi%C3%B3n_Web.pdf> [Consulta: 28 de diciembre de 2016]

[289] CPLT. Amparo C967-12. Enlace directo: [En línea] < http://extranet.consejotransparencia.cl/Web_SCW/Archivos/C967-12/C967-12_Decisi%C3%B3n_Web.pdf > [Consulta: 28 de diciembre de 2016]

así que concurre en estos casos la autorización legal en los términos exigidos por la norma para que la información médica concerniente a un menor de edad pueda ser entregada tanto a su madre como a su padre. [290]

i.b) Antecedentes de matrícula de hija menor de edad y la información sobre sus asistencias e inasistencias al centro educacional: El CPLT ha señalado que atendida la naturaleza de la información requerida se logra desprender que los padres de la menor no hacen vida en común, entendiéndose que correspondería a la madre el cuidado personal de la hija de ambos, además de la patria potestad y la representación legal; por tanto, al ser el padre quien requiere la información y no constándole al CPLT resolución judicial o acuerdo de ambos padres respecto del cuidado de la menor por parte del padre, se logra concluir que éste no detenta la representación legal de la misma. Sin embargo, esta corporación razona también en el sentido de indicar que no resulta posible impedir a un padre conocer la información relativa a antecedentes personales y/o sensibles de un menor, específicamente datos relativos a la situación educacional, existiendo por ende, la autorización legal en los términos que exigen los artículos 4 y 7 de la Ley Nº 19.628 para que la información requerida

[290] CPLT. Amparo C832-13. Enlace directo: [En línea] <http://extranet.consejotransparencia.cl/Web_SCW/Archivos/C832-13/C832-13_Decisi%C3%B3n_Web.pdf > [Consulta: 28 de diciembre de 2016]

de la menor de edad pueda ser entregada tanto al padre como a la madre de la misma.[291]

i.c) Copias de actas resolutivas del Consejo de Profesores sobre las razones para resolver y determinar la sanción reglamentaria de condicionalidad de matrícula del hijo menor de edad: Revisado los antecedentes el CPLT determina que dado que el acta de sesión del Consejo de Profesores del establecimiento educacional público contiene datos personales del hijo del requirente, se colige que éste ha hecho uso del denominado habeas data impropio en representación de su hijo a efectos de acceder a los datos de carácter personal que obran en poder de un tercero. Cabe señalar que en aquellos casos en que lo solicitado contenga datos personales de menores distintos al hijo del reclamante, el órgano público deberá aplicar el principio de divisibilidad consagrado en el artículo 11 letra d) de la Ley de Transparencia procediendo al resguardo de la información de terceros, previo a la entrega del documento requerido a quien acredite ser el representante legal del menor; en este sentido se recalca además que la entrega de la información procederá sólo en la medida que el padre tenga la representación legal de su hijo en virtud de la legislación vigente, cuestión que el órgano público reclamado deberá verificar conforme al punto 4.3 de la Instrucción General Nº 10 del Consejo para la

[291] CPLT. Amparo C967-12. Enlace directo: [En línea] <http://extranet.consejotransparencia.cl/Web_SCW/Archivos/C967-12/C967-12_Decisi%C3%B3n_Web.pdf > [Consulta: 29 de diciembre de 2016]

Transparencia,[292] esto es, entrega presencial con acreditación de calidad de padre.

ii) Denuncias en que intervienen menores de edad [293]

ii.a) Copia de denuncia y de investigación eventualmente realizada por la Junta Nacional de Auxilio Escolar y Becas e información de Beca de Integración Territorial – BIT - de la que es beneficiaria la hija del solicitante, suspendida por denuncia de un concejal: En este caso, la reclamante conoce la identidad del denunciante, por tanto el análisis se centra en la publicidad del contenido de la denuncia y la investigación que con ocasión de la misma se realizó. El CPLT sostiene que en el caso de reclamos o denuncias presentados por autoridades públicas o por funcionarios públicos en ejercicio de su cargo o función pública, no puede alegarse que la revelación de sus identidades fuese a causarles algún perjuicio, de manera que si la denuncia o reclamo se efectúa invocando una función de esta naturaleza o detentando la calidad de autoridad la identidad deberá ser revelada sin más, entregando los nombres completos. Al conocer el reclamante el nombre del denunciante y al tratarse éste de un servidor público,

[292] CPLT. Amparo C1562-12. Enlace directo: [En línea] < http://extranet.consejotransparencia.cl/Web_SCW/Archivos/C1562-12/C1562-12_Decisi%C3%B3n_Web.pdf > [Consulta: 29 de diciembre de 2016]

[293] Roles: C781-10; C265-12; C117-13; C2428-16; y C1520-16); Decisiones disponibles en www.cplt.cl, a través de la siguiente ruta: Portada / Banner "Seguimiento de Casos". Vínculo directo de ingreso: http://www.consejotransparencia.cl/consejo/stat/search/search_results.html?filtro_busqueda=seguimiento

el amparo fue acogido y se ordenó a la JUNAEB la entrega de la denuncia presentada; ello, sin perjuicio de ordenar se tarjen los datos de carácter personal que éste pudiera contener, salvo en relación al domicilio de la beneficiaria – estudiante, hija del reclamante -, por cuanto a juicio del CPLT, en este caso, se trata de un dato necesario para comprobar uno de los requisitos para otorgar el beneficio de la Beca de Integración Territorial.

Señala el CPLT que en aquellos casos en que el solicitante desconozca el nombre del denunciante, éste no podrá ser entregado pues se trata de un dato personal del cual aquel es titular; por ende, y de acuerdo a lo establecido en el artículo 4 de la Ley N° 19.628, sólo con el consentimiento expreso de su titular se puede entregar o publicar, a menos que se obtenga de una fuente accesible al público o la ley expresamente lo autorice, cuestión que en el amparo en cuestión no ocurre, pues los datos personales de los niños que son tratados en el sistema educacional no pueden considerarse como provenientes de fuentes de acceso al público para proceder a su revelación y merecen protección pese a las falencias de nuestra legislación en la materia.[294]

ii.b) Informes de denuncias sobre maltrato del profesor del establecimiento educativo: En este caso, los terceros involucrados fundaron su oposición a la

[294] CPLT. Amparo C781-10. Enlace directo: [En línea] <http://extranet.consejotransparencia.cl/Web_SCW/Archivos/C781-10/C781-10_decision_web.pdf > [Consulta: 29 de diciembre de 2016]

entrega de la información argumentando en que los antecedentes requeridos podrían ser utilizados como mecanismos de hostigamientos y represalias en contra de un menor de edad que aún se mantienen en el establecimiento educacional y porque los hechos denunciados han afectado al estado de salud del estudiante, quien se mantiene en tratamiento psiquiátrico, afectando también la seguridad física e integridad síquica de los hermanos. Ante ello el CPLT determina que el acceso al nombre de él o los denunciantes puede conllevar a que aquellos que pretendan efectuar futuras denuncias ante los órganos y servicios de la Administración del Estado se inhiban de realizarlas, impidiendo con ello que tales órganos y servicios cuenten con un insumo inestimable que les sirva de base para efectuar las fiscalizaciones necesarias destinadas a esclarecer los hechos o irregularidades de que éstas puedan dar cuenta (Art. 21 N° 1 Ley de Transparencia)

A mayor abundamiento, el CPTL considera que entregar dichos informes expondría a los menores de edad al conocimiento público de situaciones relativas a su esfera de privacidad, representando un daño presente, probable y específico a su intimidad que configuraría la causal de reserva contemplada en el artículo 21 N° 2 de la Ley de Transparencia y en lo dispuesto en el artículo 16.1 de la Convención de Derechos del Niño.[295] Por tanto, se representa al

[295] Artículo 16.1 Convención de Derechos del Niño: "*ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o correspondencia, ni de ataques ilegales a su honra o reputación".*

órgano reclamado que frente a futuros requerimientos de información referidos a denuncias, debe abstenerse de remitir los datos personales de contexto de los denunciantes en el caso de los solicitantes que no se manifestasen acerca de la entrega de la información en los términos establecidos en el artículo 20 de la Ley de Transparencia y el artículo 7 de la Ley N° 19.628, debiendo entonces, previo a la entrega de la información, tarjar aquellos datos personales proporcionados por los denunciantes para los fines específicos y no para su cesión a terceros, en virtud del principio de divisibilidad previsto en la Ley de Transparencia.[296]

ii.c) Copia de toda denuncia, expedientes, resoluciones y sanciones dictadas por la Superintendencia de Educación Escolar y que digan relación con una discriminación por orientación sexual: Señala el CPLT que dentro de las funciones de la Superintendencia de Educación Escolar está la de atender denuncias y reclamos de los miembros de la comunidad educativa, y que para desarrollar sus labores de fiscalización en materia de discriminación deben necesariamente dotar de protección y reserva a las víctimas de conductas atentatorias a su dignidad. Si bien lo solicitado refiere a la totalidad de expedientes debidamente anonimizados, divulgar la información requerida supone necesariamente restar efectividad a las labores que ella cumple

[296] CPLT. Amparo C265-12. Enlace directo: [En línea] <http://extranet.consejotransparencia.cl/Web_SCW/Archivos/C265-12/C265-12_Decisi%C3%B3n_Web.pdf> [Consulta: 29 de diciembre de 2016]

respecto del cuidado y protección de los niños y niñas vulneradas, por cuanto podrían inhibirse no sólo de ingresar denuncias por concepto de discriminación, sino también a colaborar con su testimonio en procesos en que se vean involucrados, razón por la que se rechaza el amparo con el objetivo de proteger los antecedentes personales y sensibles de los menores involucrados, tarea esencial de la Superintendencia de Educación Escolar.[297]

iii) Información concerniente a alumnos de establecimientos de educación [298]

iii.a) Información por colegios, con lista de alumnos y datos de nombres, run, edad, fecha de ingreso al establecimiento e indicación de si son o no beneficiarios por la ley SEP[299]: El CPLT sostiene que el artículo 21 N° 2 de la Ley de Transparencia otorga protección a las personas respecto de derechos y no de simple interés; por ende, para verificar la procedencia de una causal de reserva es necesario determinar la afectación de alguno de los derechos subjetivos protegidos por ella, debiendo entonces acreditarse una expectativa

[297] CPLT. Amparo C1520-15. Enlace directo: [En línea] <http://extranet.consejotransparencia.cl/Web_SCW/Archivos/C1520-15/Decision_Web_C1520-15.pdf> [Consulta: 30 de diciembre de 2016]

[298] Roles: C906-10; C925-10; C284-12 y C286-12; y C2662-14; Decisiones disponibles en www.cplt.cl, a través de la siguiente ruta: Portada / Banner "Seguimiento de Casos". Vínculo directo de ingreso: http://www.consejotransparencia.cl/consejo/stat/search/search_results.html?filtro_busqueda=seguimiento

[299] Ley de Subvención Escolar Preferente, Ley N° 20.248 de 2008.

razonable de daño presente, probable y con suficiente especificidad para justificar su reserva; lo solicitado es parte de la vida privada de los alumnos, constituyendo datos personales de los mismos que el servicio público debe resguardar, sobretodo en consideración a la especial protección que nuestro sistema jurídico otorga a los menores de edad, en armonía con la Convención de Derechos del Niño. La información sobre datos personales de un menor de edad no podrá ser tratada si no es de conformidad a las reglas y principios del tratamiento de datos en su aplicación a los calificados como sensibles, por tanto, de acuerdo al artículo 10 de la Ley N° 19.628 no pueden ser objeto de tratamiento, salvo que una ley lo autorice, exista consentimiento del titular – representante legal – o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares; [300] en consecuencia, el CPLT determina rechazar el amparo presentado.

iii.b) Listado de niños favorecidos con la entrega de uniformes escolares por parte del Ministerio de Educación: El CPLT haciendo análisis de las normas y respecto de las solicitudes de nómina de beneficiarios de becas otorgadas por órganos públicos del ámbito educación, decide rechazar el amparo, pues de acuerdo a la Convención de Derechos del Niño, específicamente su artículo 16.1., al realizar un test de daño y evaluando los bienes jurídicos en juego, se

[300] CPLT. Amparo C2662-14. Enlace directo: [En línea] <http://extranet.consejotransparencia.cl/Web_SCW/Archivos/C2662-14/Decision_Web_C2662-14.pdf> [Consulta: 30 de diciembre de 2016]

determina que la transparencia del otorgamiento de las subvenciones por parte del órgano requerido por una parte, y el respeto a la protección de la vida privada de los menores de edad por otra, no permite la revelación de la información relativa a la nómina de los alumnos solicitada, pues los expondría al conocimiento público respecto de situaciones relativas a la esfera de su privacidad, lo que representa un daño presente, probable y específico al bien jurídico indicado.

Razona la decisión que sin perjuicio de lo indicado, y en atención al artículo 1.9. de la Instrucción General N° 11, al regular la obligación de publicar la nómina de los beneficiarios de los programas sociales en ejecución por los órganos de la Administración del Estado, no se debe individualizar a los beneficiarios cuando ello suponga la revelación de datos sensibles, pues en tales casos deberá informarse el número total de beneficiarios y razones fundadas de la exclusión de la nómina.[301]

[301] CPLT. Amparo C906-10. Enlace directo: [En línea] <http://extranet.consejotransparencia.cl/Web_SCW/Archivos/C906-10/C906-10_decision_web.pdf > [Consulta: 30 de diciembre de 2016]

iv) Divulgación de datos personales de menores por parte de órganos públicos [302]

iv.a) Planes de educación media formación diferenciada humanística-científica de 3° y 4° medios: Revisados los antecedentes que obran en el expediente y teniendo en cuenta la realización de gestión oficiosa, se logra determinar que las actas remitidas al reclamante por el Ministerio de Educación – MINEDUC -, y las copias de las actas digitales del registro de calificaciones finales y promoción de los alumnos de 3° A y 4° A de Educación Media del colegio requerido, contienen datos personales de los alumnos, tales como nombre, RUT, fecha de nacimiento y sus calificaciones, así como también el nombre completo y RUT de los profesores de dichos cursos, datos que no han sido resguardados por la reclamada al momento de proporcionar la información pedida de conformidad a lo establecido en el artículo 4 de la Ley N° 19.628, especialmente en consideración a que se trata de datos de menores de edad.

En este sentido, y tal como se indicó anteriormente, los datos tratados en el sistema educacional no pueden ser considerados como provenientes de fuente accesible al público para proceder a su revelación y merecen protección,

[302] Roles: 392-12 y C426-16; Decisiones disponibles en www.cplt.cl, a través de la siguiente ruta: Portada / Banner "Seguimiento de Casos". Vínculo directo de ingreso: http://www.consejotransparencia.cl/consejo/stat/search/search_results.html?filtro_busqueda=seguimiento

especialmente considerando que uno de los principios de nuestra legislación es el interés superior del niño.

Atendida la entrega de información que contiene datos personales de menores por parte del MINEDUC, el CPLT representa severamente el no haber dado adecuada protección a los datos personales que debe cautelar, por lo que se requirió que en lo sucesivo adopte todas las medidas para evitar esta situación se repita.[303]

iv.b) Información del día, lugar, hora aproximada, niño o niños afectados y descripción de los hechos que constituyen malos tratos en jardín infantil: Al respecto el CPLT constata que la información requerida fue entregada a la reclamante; sin perjuicio de ello el órgano garante del acceso a la información, entendiendo que los antecedentes consultados son datos personales de sus titulares y no constando en el procedimiento que se haya prestado anuencia a la entrega de identidad u otros datos personales que puedan estar contenidos en los registros que obren en poder de la reclamada de conformidad a lo dispuesto en el artículo 4 de la Ley N° 19.628, ni tampoco que exista un interés público prevalente que justifique su divulgación, determina que no resulta plausible acceder a la entrega de la información.

[303] CPLT. Amparo C392-12. Enlace directo: [En línea] <http://extranet.consejotransparencia.cl/Web_SCW/Archivos/C392-12/C392-12_Decisi%C3%B3n_Web.pdf > [Consulta: 30 de diciembre de 2016]

Respecto a la entrega efectuada se representa al servicio el haber entregado la información pedida, por cuanto la publicidad de dicha información podría provocar un perjuicio a los sujetos titulares de los derechos eventualmente vulnerados, es decir, a los menores de edad involucrados; sostiene el CPLT que atendida que la revelación de la identidad de la parte recurrente da cuenta de la circunstancias de que fue denunciado ante el servicio requerido por hechos que constituirían malos tratos a menores de edad, se considera es un dato que se debe proteger, razón por la que se ordena la reserva de dicha identidad en los registros internos del CPLT y además en la información sobre procesos en cursos disponibles en la página web de la corporación fiscalizadora.[304]

Finalmente, importante señalar en este capítulo que, al momento de escoger la jurisprudencia tanto del INAI, la AEPD y el CPLT, se tuvo en consideración las materias más consultadas a los órganos públicos educacionales y que tenían por protagonistas a niñas, niños y adolescentes, apuntando los requerimientos, de una u otra manera, a sus datos personales y/o sensibles.[305] Es así que se procedió a esquematizar las solicitudes conforme a las

[304] CPLT. Amparo C426-16. Enlace directo: [En línea] <http://extranet.consejotransparencia.cl/Web_SCW/Archivos/C426-16/DecisionWeb_C426-16.pdf> [Consulta: 30 de diciembre de 2016]

[305] Indicar que también se ha aludido a estudiantes universitarios para referirnos a la cancelación de datos personales.

resoluciones de los órganos garantes y específicamente a la forma cómo éstos analizaron y determinaron la protección de los datos de sus titulares.

En cuanto a las conclusiones respecto de la jurisprudencia chilena y la comparada, valga indicar – sin perjuicio de la conclusión final de esta tesis - que existe uniformidad en el entendimiento y tratamiento sobre qué antecedentes de los menores de edad deben ser protegidos – por ejemplo, antecedentes de salud o antecedentes académicos -, adoptando cada uno de los países en análisis distintas alternativas de resguardos en pro de cumplir con sus respectivas leyes de protección de datos personales: en ciertos casos se opta por tarjar datos, en otras por no incluir los antecedentes en los sitios web de la institución para no divulgar lo que pretende mantenerse en reserva, y en otros denegar el requerimiento alegando la afectación de sus derechos a la vida privada.

Por su parte, la diferencia elemental en cada una de ellas es la presencia, autoridad y eficacia del órgano de control, cuestión ya resuelta en México como en España. En cuanto a Chile, y que como ya se indicó reiteradamente– y a pesar de la cantidad de años que han transcurrido - aún está en discusión y tramitación parlamentaria la creación e implementación de una autoridad de control en materia de protección de datos, lo que en definitiva dificulta el análisis y profundización en problemáticas de relevancia al carecer de las atribuciones

legales que una tarea como la de “decir el derecho” requiere; sin perjuicio de ello, es posible establecer que el Consejo para la Transparencia en su labor de fiscalización respecto de órganos públicos da pasos sigilosos, pero firmes en la intención de proteger los datos personales, lo que ha generado de una u otra manera “jurisprudencia” que con el paso del tiempo y a falta de la respectiva institucionalidad, ha sido adoptada por los servicios públicos, cumpliéndose el mandato legal de la Ley Nº 19.628 que de otra forma, acabaría siendo letra muerta en nuestro ordenamiento jurídico.

CONCLUSIONES

Efectuado el análisis de la protección de datos en la actual legislación nacional y su símil española y mexicana es posible colegir diversas conclusiones que, lastimosamente para nuestro país no se presentan como auspiciosas, puesto que se presenta un escenario con débil protección, específicamente tratándose de datos personales de niños, niñas y adolescentes. Si bien existen esfuerzos legislativos en torno a una mejora de la ley actual, no existen leyes sectoriales, en este caso de educación, que permitan su debida protección en forma expresa, lo que podría traducirse en que eventualmente no exista un amparo efectivo de sus derechos.

De acuerdo al examen realizado sobre el derecho comparado, cabe sostener que tanto en España como en México, y al igual como sucede en nuestro país, nada mencionan en sus leyes de protección de datos personales sobre los derechos de menores. Sin embargo, la diferencia principal con nuestra legislación radica en que tales países si han desarrollado un sistema de protección de las niñas, niños y adolescentes en cuerpos normativos distintos, aunque vinculados a las normas ya aludidas.

Concretamente en el país del norte se ha dispuesto la Ley para la Protección de los Derechos de Niñas, Niños y Adolescentes, aludiendo específicamente a los derechos de este segmento de la población, armonizándose de esta manera la Ley General de Educación que se remite a la Ley para la Protección de los Derechos citada para brindarles protección. Por su parte España remite el resguardo a datos personales de menores a su Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos, en el que se especifican los casos en que es necesario recabar el consentimiento de menores para el tratamiento de sus datos personales. En consecuencia, los cuerpos legales citados confieren y garantizan a los menores el derecho a la intimidad personal y familiar y a la protección de sus datos personales, disponiendo de forma expresa que no podrán ser objeto de injerencias arbitrarias e ilegales en su vida privada, su familia, su domicilio o correspondencia y que se necesitará de su consentimiento – atendiendo a la edad del o la menor – y de su opinión para tratar sus datos personales y/o sensibles.

En el caso de nuestro país, la Ley General de Educación, Ley Nº 20.370, aún cuando es producto de la evolución necesaria del sistema y del ajuste que periódicamente va disponiendo el ordenamiento jurídico en sus distintas aristas y en virtud de la naturaleza de las materias propias de esta área, no ha previsto protección especial de datos personales respecto de los niñas, niños y adolescentes.

El mencionado texto legal, establece una serie de derechos y deberes tanto del Estado como de los padres y la comunidad, describiendo una serie de derechos que permiten que la actividad educativa se desarrolle dentro de un marco regulatorio que pareciera ser eficaz, pero no refiere específicamente al derecho a protección de datos personales; en consecuencia, es posible arribar a una primera conclusión relativa a que el legislador no dispuso ningún precepto legal expreso o explícito que atienda y ampare los datos personales, menos aún los datos sensibles de los menores, dejando con ello – a primera vista - desprovisto de protección un ámbito tan complejo y delicado como los antecedentes de quienes conforman el segmento estudiantil.

Sin perjuicio de lo señalado, y de una lectura un poco más acabada de la Ley General de Educación, pareciera conveniente detenerse en dos artículos del Párrafo 2º, de los cuales podría deslizarse cierta protección en materia de datos personales.

A saber:

a) En primer lugar, el artículo 4, inciso séptimo de la ley en comento señala que el Estado debe resguardar los derechos de los padres y alumnos. En este caso, si bien la norma transcrita no alude expresamente a datos personales, en un sentido amplio sí podrían ser abordados, pues refiere “derechos” de padres y “alumnos”, sin enumerar alguno (s) en particular, lo que daría pie a entender

que se trata de todo derecho que encontremos en la ley y consecuentemente también en la Constitución Política; de esta manera sería posible establecer –aunque forzosamente - que a través de la Ley Nº 20.370 se protegen los derechos de niñas, niños y adolescentes en lo que respecta a su intimidad o vida privada.

b) En segundo lugar, de la norma de educación, específicamente de su artículo 1 también parecería deslizarse cierta “garantía” a la protección de la vida privada del menor o la menor, al establecer que, sin perjuicio de los derechos y deberes que establecen las leyes y reglamentos, los integrantes de la comunidad educativa, específicamente los alumnos y las alumnas, gozarán, entre otros, de los siguientes derechos: Derecho a recibir una educación que les ofrezca oportunidades para su formación y desarrollo integral; a no ser discriminados arbitrariamente; a estudiar en un ambiente tolerante y de respeto mutuo, a expresar su opinión y a que se respete su integridad física, y moral, no pudiendo ser objeto de tratos vejatorios o degradantes y de maltratos psicológicos. Tienen derecho, además, a que se respeten su libertad personal y de conciencia, sus convicciones religiosas e ideológicas y culturales, conforme al reglamento interno del establecimiento.

A este respecto, se realzan algunos conceptos, por la vinculación con la Ley Nº 19.628 en relación con las niñas, niños y adolescentes que integran la comunidad escolar:

a) Derecho a no ser discriminado arbitrariamente: Importantísima arista al momento del tratamiento de datos de menores, pues el manejo de datos personales y/o sensibles permiten la elaboración de perfiles de preferencia o bien de discriminación que potencialmente podrían significar vulneración de los derechos de los menores al segregárseles por el hecho de hacerse público algún antecedente que pertenezca a su vida privada.

b) Derecho al respeto y a la integridad física y moral de los menores: En este punto se centra la atención en la integridad física y moral de los menores que pudieran verse afectados por intromisión en su vida íntima. Si bien no es texto expreso, cabría vincular este precepto con la Ley de Transparencia,[306] específicamente con su artículo 21 Nº 2, que dispone que las únicas causales de secreto o reserva en cuya virtud pueden denegarse total o parcialmente el acceso a la información tendrá lugar cuando la publicidad, comunicación o conocimiento afecte los derechos de las personas, particularmente tratándose de – entre otros - la esfera de la vida privada. En consecuencia, vinculando la Ley Nº 20.370 con la Ley Nº 19.628, podríamos sostener que existiría

[306] Artículo Primero de la Ley Nº 20.285 que aprueba la Ley de Transparencia de la función pública y de acceso a la información de la Administración del Estado.

protección de los datos personales de menores si consideramos que el artículo 1 de la ley en comento dispone que si bien toda persona puede efectuar el tratamiento de datos personales, debe hacerlo de manera concordante con la ley y para finalidades permitidas por el ordenamiento jurídico, respetando siempre el pleno ejercicio de los derechos fundamentales de los titulares de los datos y las facultades que tal ley les reconoce. Por ende, al hablar de establecimientos de educación, cada tratamiento de datos que realice respecto de los menores – como de apoderados, personal docente y administrativo, y otros – debe ser con estricto apego a la ley, ponderando siempre las eventuales lesiones que pudieran provocar a los derechos fundamentales, entre los cuales evidentemente se ubica la intimidad de cada uno de los ellos.

c) Derecho al respeto a la libertad personal y de conciencia, de las convicciones religiosas e ideológicas y culturales de los menores: En este sentido podemos señalar que la Ley Nº 20.370 expresamente refiere una garantía y protección a aspectos de carácter personal y sensible de quienes componen la comunidad escolar, y específicamente de los menores; respeto referido a la necesidad de reserva de datos sobre opciones religiosas de éstos a terceros ajenos a su entorno familiar y/o académico, donde sólo se permitirá su revelación en caso de consentimiento de quienes ostenten calidad de padre, madre y/o apoderado. Misma situación es la relativa a las convicciones ideológicas y culturales, como por ejemplo pertenecer a alguna etnia en

particular, o algún pueblo originario; ello por la esencia misma del respeto a ese antecedente como por la necesidad de evitar discriminaciones arbitrarias conforme a lo señalado precedentemente.

Una segunda conclusión de la presente tesis – que puede desprenderse de la ya esbozada - es que nuestra Ley Nº 19.628 tanto en su elaboración como en implementación, regula el tratamiento de datos, mas no el derecho efectivo de los titulares, ello puesto que pareciera ser que los derechos que ella disponen no son más que meras declaraciones de voluntad del legislador en atención a que las herramientas para su garantía no son expeditas, muchas veces son costosas y sometidas a un procedimiento que no es del todo garante. Consecuencia de lo indicado es que en caso de darse a conocer un dato personal y / o sensible en virtud de un mal tratamiento en un establecimiento de educación, es muy probable que el apoderado de ese o esa menor desconozca el procedimiento de reparo de tal vulneración y eventualmente no disponga los medios para contar con asesoría al respecto, lo que se traducirá en que el derecho no será ejercido, y por ende no habrá una real protección del derecho a la intimidad del o la menor involucrada, como tampoco sanción a quien ha irrespetado la normativa de datos personales.

En lo que respecta al órgano garante, considerando la realidad mexicana, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales se alza como el ente encargado de velar por la protección de datos personales, hecho relativamente nuevo que permitió que el antiguo Instituto (IFAI), además de constituirse como el protector del derecho de acceso a la información, se transformara en el garante de los datos personales y sensibles de las personas, lo que significó la ampliación de las atribuciones conferidas por ley, la asignación de recursos y la infraestructura necesaria para permitirle diligenciar adecuada y correctamente esta tarea. Luego en España, la Agencia Española de Protección de Datos es la entidad ante la cual se reclama respecto de órganos públicos como privados las reclamaciones por afectación de los derechos a la privacidad, generándose al respecto variada jurisprudencia en torno a los procedimientos que se disponen para la protección de la vida privada, reconociéndose expresamente a los titulares los derechos ARCO, garantizando consecuencialmente con ello el derecho a la vida íntima de los menores de edad.

En este punto se refleja claramente la posición de desventaja que en la materia ostenta nuestro país respecto de los otros que conforman parte de, por ejemplo, la OCDE o de la Comunidad Iberoamericana, básicamente en atención a que tales entidades realzan la importancia de contar con un órgano garante de la protección de datos, que sea capaz de determinar responsabilidades

respecto de infracciones a la normativa y aplicar las sanciones que establezca la ley.

Chile se queda atrás en estos lineamientos, discutiendo recién cuál será la entidad que tomará esta tarea en sus manos: Consejo para la Transparencia v/s Dirección Nacional de Protección de Datos Personales (Ministerio de Hacienda). Interesante en este punto señalar que en caso de ser ésta última la entidad aprobada por el Congreso, podría resultaría dudosa la independencia que ostente en los términos planteados en el proyecto de ley impulsado por la Presidenta de la República, pues al instituirse a un órgano de la Administración del Estado podría verse mermada la independencia que exigen los estándares internacionales ya aludidos, al “relacionarse” mediante otros órganos de la Administración del Estado, amén de las posibles discrepancias que pudieran existir con el Consejo para la Transparencia relativas a la interpretación de los derechos en juego.

En este escenario sería conveniente que al momento de la implementación de la nueva normativa de protección de datos personales que se dicte se contemplen, por ejemplo, las directrices OCDE, lo que se traduce en que el esfuerzo debe redoblarse para así alcanzar y calzar con estándares internacionales que nos posicionen a un nivel de confianza y eficacia mayor al actual respecto del resto de los países que conforman esta Organización y

sobretodo permitan garantizar, especialmente, que los derechos de las niñas, niños y adolescentes puedan ser tutelados a través de un procedimiento expedito y claro ante una entidad con la suficiente independencia al momento de decidir el derecho.

Como tercera conclusión, sin perjuicio de lo señalado precedentemente en cuanto a la distancia legal – y constitucional – que en la materia nos separa de México y España, cabe precisar que las diferencias no parecieran ser tales en cuanto a lo que ha intentado realizar el Consejo para la Transparencia dentro de su atribución legal de velar por el adecuado cumplimiento de la Ley Nº 19.628 respecto de organismos públicos. En este ámbito las decisiones del CPLT no resultan ser tan diferentes a los razonamientos y conclusiones a las que han arribado el INAI o la AEPD, puesto que en virtud del análisis efectuado, por materias o categorías de materias, sus fundamentaciones resultan bastantes similares al momento de proteger los datos personales de niñas, niños o adolescentes. A modo de ejemplo, se coincide en que los datos contenidos en evaluaciones psicopedagógicas y psicológicas de los menores son de naturaleza sensible y por ende es menester resguardarlos con mayor cautela, de conformidad a las legislaciones nacionales como a la Convención sobre los Derechos del Niño, a la que adhieren los países analizados.

Otro ejemplo es el acceso a información por parte de progenitor no custodio de antecedentes curriculares educativos o de salud de un o una menor, instancia en que los tres órganos garantes en análisis discurren en mismo razonamiento, esto es, en atender el requerimiento de padre o madre no custodio respecto de los antecedentes personales y/o sensibles de su hija o hijo menor de edad, puesto que no resulta posible impedir a un padre o una madre conocer la información relativa a antecedentes personales y/o sensibles de un o una menor, específicamente datos relativos a la situación educacional, puesto que se configura la autorización legal exigida por los ordenamientos jurídicos para que la información requerida de los menores de edad pueda ser entregada tanto al padre como a la madre de los mismos.

En cuanto al consentimiento y competencias, si bien la redacción de las normativas de cada país pudiera inducir a la confusión sobre la forma de prestar el consentimiento, la lectura exhaustiva de las mismas permite colegir su semejanza; mientras en Chile la norma señala que éste debe ser expreso; en España, que el consentimiento debe ser inequívoco. Se trata entonces de una misma forma de prestar el consentimiento, puesto que la doctrina cuando habla de consentimiento expreso se exige que sea declarado en forma clara y inequívoca, mediante la expresión de la voluntad, mientras que el consentimiento inequívoco refiere a que no resulta admisible deducir el consentimiento de los meros actos realizados por su titular, es decir, no tiene

cabida el consentimiento tácito, siendo menester que exista expresamente una acción u omisión que implique la existencia de ese consentimiento. Por su parte, en cuanto a la competencia, las normas son casi idénticas al indicarse que no será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus atribuciones.

En síntesis, nuestra legislación se encuentra “al debe” en la protección de datos personales respecto de los menores pues no existen normas sectoriales expresas que nos permitan garantizar en forma directa los derechos de la población estudiantil menor de edad; sin perjuicio de lo que podría ser garantizado en forma indirecta. No obstante, la buena nueva es que existen esfuerzos por mejorar la legislación existente, por sustentar e implementar estándares internacionales que nos lleven a situarnos como país de confianza en estos ámbitos, tanto en lo que dice relación con el procedimiento, como con lo que respecta al órgano garante, y en este sentido en Chile el camino ya está pavimentado, debiendo continuarse en esta senda para lograr definitiva y efectivamente el respeto, protección y garantía a la vida privada de niñas, niños y adolescentes.

BIBLIOGRAFÍA CONSULTADA

TRATADOS, INSTRUMENTOS E INFORMES INTERNACIONALES

- COMITÉ DE DERECHOS ECONÓMICOS, SOCIALES Y CULTURALES, establecido en virtud de la Resolución 1985/17, de 28 de mayo de 1985, del Consejo Económico y Social de las Naciones Unidas.

- CONSEJO DE EUROPA. 2014. Manual de legislación europea en materia de la protección de datos. Agencia de los Derechos Fundamentales de la Unión Europea.

- CONVENCIÓN DE DERECHOS DEL NIÑO, 1989, Naciones Unidas.

- CONVENIO DEL CONSEJO EUROPEO N° 108 PARA LA PROTECCIÓN DE LAS PERSONAS, con respecto al Tratamiento Automatizado de Datos de Carácter Personal de 1981.

- DIRECTIVA 95/45/CE del Parlamento Europeo y del Consejo del 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

- GRUPO DE TRABAJO 29 – GT29- 2010.

- INFORME JURÍDICO, Agencia Española de Protección de Datos 445/2009

- PRINCIPIOS RECTORES PARA LA REGLAMENTACIÓN DE FICHEROS COMPUTARIZADOS DE DATOS PERSONALES, Asamblea General de las Naciones Unidas. Resolución 45/95 de 14 de diciembre de 1990.

- RECOMENDACIÓN RELATIVA A LAS DIRECTRICES APLICABLES A LA PROTECCIÓN DE LA VIDA PRIVADA Y A LOS FLUJOS TRANSFRONTERIZOS DE DATOS PERSONALES, Organización de Cooperación y Desarrollo Económicos, Consejo de Ministros, 23 de septiembre de 1980.

- RECOMENDACIÓN DE LA COMISIÓN 81/670 CEE de 29 de julio de 1981, relativa al Convenio del Consejo de Europa sobre protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

- REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS 2016/679, aprobado por el Parlamento Europeo el 14 de abril de 2016, que sustituye y renueva la anterior Directiva 95/46/CE.

LEGISLACIÓN, ACTOS ESTATALES Y OTROS DOCUMENTOS

- ESPAÑA. Código Civil.

- ESPAÑA. 1992. Ley Orgánica 5/92, de Regulación del Tratamiento Automatizado de Datos.

- ESPAÑA. 1999. Ley Orgánica 15/99, de Protección de Datos de Carácter Personal.

- ESPAÑA. 2006. Ley Orgánica 2/2006 de Educación.

- ESPAÑA. 2008. Real Decreto 1720/2007 que aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de Protección de Datos de carácter personal.

- MÉXICO. Código Civil Federal Mexicano.

- MÉXICO. 1993. Ley General de Educación.

- MÉXICO. 2010. Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

- MÉXICO. 2011. Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

- MÉXICO. 2014. Ley de Protección de los Derechos de las Niñas, Niños y Adolescentes.

- México. 2017. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

LEGISLACIÓN NACIONAL

- Constitución Política de la República. 1980.

- Código Civil.

- Historia de la Ley Nº 19.628.

- Ley Nº 19.628 sobre Protección de la Vida Privada, 1999.

- Ley Nº 20.285 sobre Acceso a Información Pública, 2008.

- Ley Nº 20.370 sobre Educación General, 2009.

- DECRETO CON FUERZA DE LEY Nº 779, que aprueba Reglamento del registro de banco de datos personales a cargo de organismos públicos. Fecha de promulgación: 24 de agosto de 2000. Santiago, Chile.

- DECRETO N° 83. Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos. Fecha Publicación: 12 de enero de 2005. Ministerio Secretaria General de la Presidencia. Santiago, Chile.

- DECRETO CON FUERZA DE LEY Nº 2, que fija texto refundido, coordinado y sistematizado de la Ley N° º 20.370 con las normas no derogadas del Decreto con Fuerza de Ley Nº 1, de 2005. Fecha de promulgación: 16 de diciembre de 2009. Santiago, Chile.

SITIOS WEBS

- ABANLEX. Información sobre la AEPD, 2016. España. [En línea] <https://www.abanlex.com/areas-de-practica/proteccion-de-datos/adecuacion-lopd/agencia-espanola-de-proteccion-de-datos/> [Consulta: 20 de septiembre de 2016]

- ABERASTURI, U., 2011. Los Principios de la Protección de Datos aplicados en la Sanidad. Tesis presentada para la obtención del grado de Doctor en Derecho, Departamento de Derecho Administrativo, Constitucional y Filosofía del Derecho de la Universidad del País Vasco-Euskal Herriko Unibertsitatea, España. Pág. 196. [En línea] <https://addi.ehu.es/bitstream/10810/7664/17/ABERASTURI%20GORRI%C3%91O.pdf> [Consulta: 20 de agosto de 2016]

- AEDO, C., 2016. Educación en Chile: Evaluación y Recomendaciones de Política, Chile. Pág. 2. [En línea] <http://fen.uahurtado.cl/wp-content/uploads/2010/07/inv125.pdf **>** [Consulta: 10 de junio 2016]

- AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA, 2014. Manual de legislación europea en materia de la protección de datos. Consejo de Europa. Pág. 77. [En línea] <http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-es.pdf> [Consulta: 08 de agosto de 2016]

- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. 2017. Videovigilancia en los colegios, Informe del Gabinete Jurídico, España. Págs. 6 y 7. [En línea] <https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/videovigilancia/common/pdfs/2006-0262_Videovigilancia-en-los-colegios.pdf> [Consulta: 21 de agosto de 2016]

- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Canal del responsable de ficheros. Deber de Información. España. [En línea] <https://www.agpd.es/portalwebAGPD/canalresponsable/obligaciones/deber_informacion/index-ides-idphp.php> [Consulta: 18 de julio de 2016]

- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía del Responsable del Fichero: Guía de Protección de datos para Responsables de Ficheros. España. [En línea] <https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_responsable_ficheros.pdf> [Consulta: 28 de julio de 2016]

- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Inscripción de Ficheros, Preguntas más frecuentes. España. [En línea] <https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/preguntas_frecuentes/cuestiones_generales/index-ides-idphp.php > [Consulta: 10 de agosto de 2016]

- AGENCIA DE PROTECCIÓN DE DATOS DE CATALUÑA. 2014. Guía básica de protección de datos para los centros educativos. Generalitat de Catalunya Autoritat Catalana de Protecció de Dades, España. Pág. 54. [En línea] < http://www.apd.cat/media/2891.pdf > [Consulta: 21 de julio de 2016]

- ÁLVAREZ, D., 2016. Acceso a la Información Pública y Protección de Datos Personales ¿Puede el Consejo para la Transparencia ser la autoridad de control en materia de Protección de Datos?. Revista de Derecho, Universidad Católica del Norte, Sección: Estudios, Año 23 N° 1, Chile. Pág. 52. [En línea] <https://dx.doi.org/10.4067/S0718-97532016000100003> [Consulta: 27 de septiembre de 2016]

- ARAYA, A., 2012. La Ley 19.628 sobre protección de datos de carácter personal y el contrato de trabajo: ¿una nueva cláusula obligatoria?. Novoa & Araya, Serie notas y artículos de interés número 2, Chile. Pág. 3. [En línea] <http://www.nyaabogados.cl/docs/NotasyArticulosNA_N2_Ley%2019628.pdf> [Consulta: 15 de julio de 2016]

- ASOCIACIÓN DE NIÑOS Y JÓVENES CON DISCAPACIDAD DE ALICANTE. ESCUELA DE FORMACIÓN E INNOVACIÓN Y ADMINISTRACIÓN PÚBLICA. 2015. Los Derechos Personalísimos. Departamento de Trabajo Social, Programa Gris "Protección Social y Acción Tutelar. Pág. 1 [En línea] < http://www.andalicante.org/enlaces/articulos-profesionales-anda/dossier-derechos-personalisimos.pdf .> [Consulta: 30 de mayo de 2017]

- BELLEI, C., 2011. La educación pública que Chile necesita. Revista "El Chile que se viene", R. Lagos y O. Landerretche, Ed., F. Democracia y Desarrollo y Ed. Catalonia, Chile. Pág. 6. [En línea] <http://www.ciae.uchile.cl/download.php?file=noticias/BELLEI%20-Chile2030.pdf. > [Consulta: 06 de julio de 2016]

- BENITO, R., 2016. Menores, DPO y nuevos principios en la Protección de Datos. Law&Trends. Best Lawyer, more Justice, España. [En Línea] <http://www.lawandtrends.com/noticias/tic/menores-dpo-y-nuevos-principios-en-la-proteccion.html> [Consulta: 12 de agosto de 2016]

- BIBLIOTECA DEL CONGRESO NACIONAL, 2013. Guía legal sobre Ley General de Educación. Detalla las novedades que trae la Ley General de Educación, que establece un marco institucional para la educación escolar. Chile. [En línea] <http://www.bcn.cl/leyfacil/recurso/ley-general-de-educacion> [Consulta: 23 de noviembre de 2016]

- BROCCA, M., 2016. El nuevo Reglamento de Protección de Datos. España. [En Línea] < https://marinabrocca.com/proteccion-de-datos/nuevo-reglamento-proteccion-datos/> [Consulta: 17 de enero de 2017]

- BURREL, B., 2014. WELIVESECURITY (en español). 10 consejos para proteger la información de instituciones educativas. [En línea] < http://www.welivesecurity.com/la-es/2014/07/08/10-consejos-proteger-informacion-instituciones-educativas/ > [Consulta: 11 de agosto de 2016]

- CENTRO DE ESTUDIOS DE DERECHO INFORMÁTICO, 2003. Derechos del Titular de Datos y Habeas data en la Ley 19.628, Revista Chilena de Derecho Informático, Facultad de Derecho, Universidad de Chile, ISNN 0717-9162. N° 2, Año 2003, Chile. [En línea]: <http://web.uchile.cl/vignette/derechoinformatico/CDA/der_informatico_simple/0,1493,SCID%253D14180%2526ISID%253D292%2526PRT%253D14178,00.html> [Consulta: 29 de junio de 2016]

- CENTRO DE ESTUDIOS EN DERECHO INFORMÁTICO, 2014. Las fuentes de acceso público en la protección de datos. Revista de Derecho y Tecnología, Vol. 3, Nro. 2, Universidad de Chile, ISSN 0719-2576, Chile. Pág. 12. [En línea] <http://www.rchdt.uchile.cl/index.php/RCHDT/article/view/33276> [Consulta: 11 de agosto de 2016]

- CENTRO DE SISTEMAS PÚBLICOS, 2010. Informe “Diseño de un modelo organizacional del Consejo para la Transparencia en su nueva función de protección de datos”, Departamento de Ingeniería Industrial, Facultad de Ciencias Físicas y Matemáticas de la Universidad de Chile, Chile. Pág. 111. [En línea] < https://datosprotegidos.org/informe-diseno-de-un-modelo-organizacional-del-consejo-para-la-transparencia-en-su-nueva-funcion-de-proteccion-de-datos/ > [Consulta: 15 de marzo de 2017]

- CERDA, A., 2006. Mecanismos de Control en la Protección de Datos en Europa. *Ius et Praxis*, *12*(2), Chile. [En línea] < https://dx.doi.org/10.4067/S0718-00122006000200009> [Consulta: 21 de septiembre de 2016]

- CONSERJERÍA DE EDUCACIÓN. 2011. Guía de Protección de datos de Carácter Personal para los Centros de Enseñanza. (Ley Orgánica 15/1999, de 13 de diciembre, y Real Decreto 1720/2007, de 21 de diciembre, Junta de Andalucía, 1° Edición, España. Pág. 80. [En línea] <http://www.juntadeandalucia.es/educacion/portalseneca/web/seneca/guia-lopd> [Consulta: 25 de agosto de 2016]

- CREEL; GARCÍA CUELLAR; AIZA Y ENRÍQUEZ., 2017. Ley General de Protección de Datos Personales. México [En línea] <http://www.creel.mx/noticias/general-law-for-the-protection-of-personal-data/> [Consulta: 30 de mayo de 2017]

- CRUZ, J., 2014. 8 Claves para entender la Agencia Española de Protección de Datos. UNIR REVISTA, España. [En línea] < http://www.unir.net/derecho/revista/noticias/8-claves-para-entender-la-agencia-espanola-de-proteccion-de-datos/549201452974/ > [Consulta: 20 de septiembre de 2016]

- CUIDA TUS DATOS. 2017. El deber de secreto en la Lopd. España. [En línea] <http://cuidatusdatos.com/obligacioneslopd/principioslopd/secreto/index.html> [Consulta: 16 de agosto de 2016]

- CUIDA TUS DATOS, 2017. El derecho a la información en la Lopd. España. [En línea] <http://cuidatusdatos.com/obligacioneslopd/principioslopd/informacion/index.html> [Consulta: 05 de agosto de 2016]

- DONOSO, L., 2009. El tratamiento de datos personales en el sector de la educación. Expansiva UDP. En Foco 136, ISSN 0717-9987, Chile. Pág. 22. [En línea] < http://www.expansiva.cl/media/en_foco/documentos/15042009150219.pdf > [Consulta: 11 de julio de 2016]

- ESCUELA DE FORMACIÓN E INNOVACIÓN Y ADMINISTRACIÓN PÚBLICA, 2015. Protección de Datos de carácter Personal: Disposiciones Generales. Datos Especialmente Protegidos. Región de Murcia. Conserjería de Hacienda y Administración Pública, España. Pág. 23. [En línea] < https://webcache.googleusercontent.com/search?q=cache:sPZpfmsaD24J:https://efiapmurcia.carm.es/web/integra.servlets.Blob%3FARCHIVO%3DC1%2520TEMA%25208.pdf%26TABLA%3DARCHIVOS%26CAMPOCLAVE%3DIDARCHIVO%26VALORCLAVE%3D117853%26CAMPOIMAGEN%3DARCHIVO%26IDTIPO%3D60%26RASTRO%3Dc%24m2813,51996,51997+&cd=3&hl=es&ct=clnk&gl=es.> [Consulta: 30 de junio de 2016]

- EQUAL PROTECCIÓN DE DATOS, 2014. La implantación de la LOPD en los colegios. España. [En línea] <https://equalprotecciondedatos.com/lopd-en-los-colegios/ > [Consulta: 11 de julio de 2016]

- ERP. 2017. Publican ley de protección de datos personales. Diario El Economista. 26 de enero de 2017. [En línea] <

http://eleconomista.com.mx/sociedad/2017/01/26/publican-ley-proteccion-datos-personales > [Consulta: 30 de mayo de 2017]

- FERNÁNDEZ, H., s.a. Los datos sensibles en la Ley de Protección de Datos Personales. Argentina. [En línea] < http://www.hfernandezdelpech.com.ar/PUBLICAtrabajosLosDatosSensEnLaLeyProteDatosPer.htm > [Consulta: 26 de agosto de 2016]

- GONZÁLEZ, A., 2016. Consentimiento para el tratamiento de datos de menores de edad. Ayuda Ley Protección de Datos. España. [En línea] < http://ayudaleyprotecciondatos.es/2016/07/28/tratamiento-de-datos-de-menores-de-edad/ > [Consulta: 18 de enero de 2017]

- GONZÁLEZ, F., s.a., Privacidad de la Información digital: autodeterminación vs. Commodity. Revista Jurídica de la Universidad de Palermo, Argentina. Pág. 77. [En línea] < http://www.palermo.edu/derecho/publicaciones/pdfs/revista_juridica/Especiales_SELA/SELA%201998%20-%20Ed%201999/04SELA98Juridica07.pdf> [Consulta: 06 de enero de 2017]

- GRUPO DE TRABAJO 29. 2008. Documento de trabajo 1/08 sobre protección de datos personales de los niños (Directrices Generales y el caso especial de los colegios). Pág. 14 [En línea] < http://www.avpd.euskadi.eus/s04-redaneto/es/contenidos/informacion/redaneto/es_redaneto/adjuntos/informe_europeo_proteccion_datos_colegios.pdf > [Consulta: 28 de agosto de 2016]

- GUTIÉRREZ, A., 2014. El Derecho a la intimidad en la era de la tecnología de las comunicaciones: Una reflexión desde el derecho constitucional. Cuestiones

Constitucionales, Revista Mexicana de Derecho Constitucional, Num. 31, México. Página 1 [En línea] < http://www.scielo.org.mx/pdf/cconst/n31/n31a8.pdf> [Consulta: 07 de enero de 2017]

- HERRÁN, A., 2002. El Derecho a la intimidad en la nueva ley orgánica de protección de datos personales. Madrid, Dykinson, España. Pág. 211. [En línea] <https://books.google.cl/books?id=CCVT48egc5MC&redir_esc=y> [Consulta: 10 de agosto de 2016]

- HUEPE, F., 2010. El Consejo para la Transparencia. Una aproximación a su funcionamiento. III Versión Seminarios, Probidad y Transparencia para la Administración, Chile. Pág. 21. [En línea] <http://www.contraloria.cl/NewPortal2/portal2/ShowProperty/BEA%20Repository/Portal/Actualidad/Actividades/Seminarios/9-10122010/Zona_sur/El_Consejo_para_la_Transparencia.pd > [Consulta: 01 de diciembre de 2016]

- INSTITUTO NACIONAL DE TRANSPARENCIA. ACCESO A INFORMACIÒN Y PROTECCIÓN DE DATOS, 2014. Estudio sobre Protección de Datos a Nivel Internacional. Iniciación sobre los modelos de bases de datos, México. Pág. 54. [En línea] <http://inicio.ifai.org.mx/Estudios/prot_datos.pdf > [Consulta: 09 de agosto de 2016]

- INSTITUTO NACIONAL DE TRANSPARENCIA. ACCESO A INFORMACIÒN Y PROTECCIÓN DE DATOS, 2014. Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, México. Pág. 59. [En línea]

<http://inicio.ifai.org.mx/nuevo/Gu%C3%ADa%20obligaciones%20de%20la%20LFPDPPP.pdf > [Consulta: 08 de agosto de 2016]

- INSTITUTO NACIONAL DE TRANSPARENCIA. ACCESO A INFORMACIÒN Y PROTECCIÓN DE DATOS, 2011. Guía práctica para generar el aviso de privacidad, México. Pág.18. [En línea] <http://inicio.ifai.org.mx/DocumentosdeInteres/privacidadguia.pdf> [Consulta: 16 de agosto de 2016]

- INSTITUTO NACIONAL DE TRANSPARENCIA. ACCESO A INFORMACIÒN Y PROTECCIÓN DE DATOS, 2014. Guía práctica para ejercer el Derecho a la Protección de Datos Personales. México [En línea] <http://inicio.ifai.org.mx/Publicaciones/01GuiaPracticaEjercerelDerecho.pdf> [Consulta: 29 de junio de 2016]

- JERVIS, P., 2006. Regulación del Mercado de Datos. Tesis para optar al grado de Magíster en Derecho. Santiago, Chile. Facultad de Derecho, Escuela de Graduados, Universidad de Chile, Chile. Pág. 83. [En línea] <http://repositorio.uchile.cl/handle/2250/114258> [Consulta: 28 de julio de 2016]

- JIJENA, R., 2013, Tratamiento de datos personales en el Estado y acceso a la información pública. Revista Chilena de Derecho y Tecnología. Centro de Estudios en Derecho Informático, Universidad de Chile. Vol. 2, Nº 2, Chile. Pág. 93. [En línea] < http://www.revistas.uchile.cl/index.php/RCHDT/article/viewFile/30309/32096>

- LÁZARO DE RAFAEL, B., 2017. Registro de un fichero de datos personales con el formulario NOTA. España. [En línea]

<http://www.adictosaltrabajo.com/tutoriales/inscripcion-fichero-datos/>
[Consulta: 25 de julio de 2016]

- MALPICA, C., 1980. Administración de la Educación y sus relaciones con la planificación y con la investigación. *R*ae Eugène-Delacroix, 75016 Paris LA, Instituto Nacional de Planeamiento de la Educación. (creado por la Unesco), Perú. Pág. 7. [En Línea]< http://unesdoc.unesco.org/images/0007/000701/070174so.pdf > [Consulta: 06 de julio de 2016]

- MARTÍNEZ, E., 2011. El Derecho a la Protección de datos Personales en la Administración Pública Federal. Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco, México. [En línea] < https://www.itei.org.mx/v3/micrositios/diplomado02/gdl/adjuntos/Sector_Publico_ITEI_18-19-nov-2011.pdf > [Consulta: 20 de enero de 2017]

- MARTÍNEZ, R., 2007. El derecho fundamental a la protección de datos: perspectivas. Monográfico: III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas». Revista de Internet, Derecho y Política, España. Pág. 50. [En línea] <http://www.uoc.edu/idp/5/dt/esp/martinez.html> [Consulta: 29 de junio de 2016]

- MAYOR, R., 2016. Contenido y Novedades del Reglamento General de Protección de Datos de la UE (Reglamento UE 2016/679, de 27 de abril de 2016). Gabilex N° 16, España. [En línea] < http://www.castillalamancha.es/sites/default/files/documentos/pdf/20160709/revista_gabilex_no_6._autor_roberto_mayor_gomez.pdf > [Consulta: 17 de enero de 2017]

- MICROSOFT. 2016. Conceptos básicos del diseño de una base de datos. [En línea] < https://support.office.com/es-es/article/Conceptos-b%C3%A1sicos-del-dise%C3%B1o-de-una-base-de-datos-eb2159cf-1e30-401a-8084-bd4f9c9ca1f5#bmpurpose > [Consulta: 10 de agosto de 2016]

- MINISTERIO DE EDUCACIÓN. Ejes claves del proyecto de ley general de educación. Chile. [En línea] <http://portales.mineduc.cl/usuarios/formacion_tecnica/File/2011/ESTUDIOS/Ejes_claves_proyecto_LGE.pdf> [Consulta: 23 de julio de 2016]

- MUÑOZ, J., 2009. Protección de datos personales en Centros Educativos públicos y privados. Privacy & Digital Business, España. [En línea] <http://www.joaquinmunoz.com/2009/05/12/proteccion-de-datos-personales-en-centros-educativos-publicos-y-privados/> [Consulta: 12 de agosto de 2016]

- NOGUEIRA ALCALÁ, H., 2008, El derecho a la educación y sus regulaciones básicas en el derecho constitucional chileno e internacional de los derechos humanos. Revista Ius et Praxis, año 14, N° 2:209-269, 2008, Chile. Pág. 210. [En línea] <http://www.scielo.cl/scielo.php?pid=S0718-00122008000200007&script=sci_arttext > [Consulta: 20 de julio de 2016]

- NUNSYS. Consultorías y Seguridad. Novedades del Nuevo Reglamento Europeo de Protección de Datos, España. Pág. 2. [En línea] < http://nunsys.com/Descargar/adaptacion-reglamento-proteccion-datos.pdf > [Consulta: 12 de agosto de 2016]

- PRIVACIDAD VS PUBLICIDAD DE LOS DATOS PERSONALES EN POSESIÓN DE AUTORIDADES. 2014. El Observatorio. México. [En línea] <

http://oiprodat.com/2014/01/23/privacidad-vs-publicidad-de-los-datos-personales-en-posesion-de-autoridades/> [Consulta: 07 de enero de 2017]

- PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN. 2012.Protec-Datos. Principio de Proporcionalidad. España. [En línea] <https://ofiseg.wordpress.com/tag/principio-de-proporcionalidad/> [Consulta: 21 de agosto de 2016]

- RAJEVIC, E., 2011. Protección de datos y transparencia en la Administración Pública Chilena. Inevitable y deseable ponderación. Expansiva UDP. En foco 162, ISSN 0717-9987, Chile. Pág 8. [En línea] <http://www.consejotransparencia.cl/consejo/site/artic/20130820/asocfile/20130820152206/protecci__n_de_datos_y_transparencia_en_la_administraci__n_p__blica_chilena.pdf> [Consulta: 11 de agosto de 2016]

- REDONDO, J; ALMONACID, C; INZUNZA, J; MENA, P.; DE LA FUENTE, L., 2007. El derecho a la educación en Chile. Colección Libros FLAPE, Chile. Pág. 10. [En línea] < http://www.opech.cl/bibliografico/Doc_Financiamiento/08Chile_Derecho.pdf > [Consulta: 24 de mayo de 2016]

- SERVICIO DE NOTIFICACIONES ELECTRÓNICAS (https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/Notificaciones_tele/index-ides-idphp.php)

- TRONCOSO, A., 2006. La publicación de datos de profesores y alumnos y la privacidad personal. Acerca de la protección de datos en las Universidades. Revista de Derecho Político, Num. 67, España. Pág. 118. [En línea]

< http://revistas.uned.es/index.php/derechopolitico/article/view/8999/8592 > [Consulta: 25 de julio de 2016]

- VALENZUELA, D., 2016. Acceso a la información pública y protección de datos personales. ¿puede el Consejo para la Transparencia ser la autoridad de control en materia de protección de datos?, Revista de Derecho, Universidad Católica del Norte, Sección: Estudios, Año 23 - Nº 1, Chile. Págs. 66, 67 y 68. [En línea] < http://www.scielo.cl/scielo.php?pid=S0718-97532016000100003&script=sci_abstract> [Consulta: 14 de septiembre de 2016]

- WIKIPEDIA. Agencia Española de Protección de Datos. <https://es.wikipedia.org/wiki/Agencia_Espa%C3%B1ola_de_Protecci%C3%B3n_de_Datos> [Consulta: 20 de septiembre de 2016]

- WIKIPEDIA. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos. [En línea]< https://es.wikipedia.org/wiki/Instituto_Nacional_de_Transparencia,_Acceso_a_la_Informaci%C3%B3n_y_Protecci%C3%B3n_de_Datos_Personales> [Consulta: 14 de septiembre de 2016]

DOCTRINA

- AGENCIA DE PROTECCIÓN DE DATOS DE LA COMUNIDAD DE MADRID. 2008. Protección de Datos Personales para Centros Educativos Públicos. Ed. 2008, España.

- ANGUITA, P., 2007. La Protección de Datos Personales y el Derecho a la Vida Privada, Régimen Jurídico, Jurisprudencia y Derecho Comparado. Análisis de la Ley N° 19.628 sobre Protección de la Vida Privada (Protección de Datos de Carácter Personal), modificada por la Ley N° 19.812. Editorial Jurídica de Chile, Chile. Pág. 543 y ss.

- DAVARA, M.A., 1998. La protección de datos en Europa. Principios, derechos y procedimiento. Madrid, Grupo Asnef Equifax, España. Pág. 24.

- INFORME DE JURISPRUDENCIA JUDICIAL, Corte Suprema, Corte de Apelaciones y Tribunal Constitucional sobre la Ley de Transparencia 2009-2016. Unidad de Defensa Judicial, Dirección Jurídica CPLT / Febrero 2017. Pág 44.

- JARAQUEMADA, J., 2015. La afectación de la vida privada como límite al Acceso a la información. Revista Transparencia y Sociedad. Edición Nº 3, Chile. Págs. 34 y 35.

- MATUS, J., 2013. Derecho de acceso a la información pública y protección de datos personales. Revista Chilena de Derecho y Tecnología, Centro de Estudios Informáticos, Universidad de Chile, Vol. 2, Nº 1, Chile. Pág. 206.

- REBOLLO, L., 2004. Derechos Fundamentales y la Protección de Datos. Madrid, Editorial Dykinson, España. Pág. 146.