consejo para la Transparencia

OFICIO Nº 000053

MAT.: Remite recomendaciones para el uso de sistemas biométricos de identificación.

ANT.: Oficio Nº 4259, de fecha 6 de septiembre de 2018, del Consejo para la Transparencia

Oficio Nº 2243, de fecha 18 de octubre de 2018, de la Junta Nacional de Auxilio Escolar y Becas

SANTIAGO, 10 ENE 2019

A: JAIME TOHÁ LAVANDEROS
DIRECTOR NACIONAL DE LA JUNTA NACIONAL DE AUXILIO ESCOLAR Y BECAS

DE: MARCELO DRAGO AGUIRRE
PRESIDENTE DEL CONSEJO PARA LA TRANSPARENCIA

Conforme a las facultades de formular recomendaciones y de velar por el adecuado cumplimiento de la Ley Nº 19.628, sobre Protección de la Vida Privada, por parte de los órganos de la Administración del Estado, establecidas en las letras e) y m) del artículo 33 de la Ley de Transparencia de la Función Pública y de Acceso a la Información de la Administración del Estado, aprobada por el artículo primero de la Ley N°20.285, y en atención a lo señalado por su institución en el Oficio N° 2243 de 2018, individualizado en el antecedente, el Consejo Directivo del Consejo para la Transparencia, en sesión N° 957, de 8 de enero de 2019, acordó remitir a usted un conjunto de recomendaciones en relación al empleo de sistemas de identificación biométrica mediante reconocimiento de huellas dactilares.

La utilización de este tipo de herramientas por parte de los organismos de la Administración del Estado constituye una materia que exige ser abordada adecuadamente, por cuanto conlleva el tratamiento de datos sensibles, relativos a las características físicas de las personas. Asimismo, en el caso particular de la Junta Nacional de Auxilio Escolar y Becas (JUNAEB), el uso de sistemas biométricos de identificación para certificar la entrega de raciones de su Programa de Alimentación Escolar (PAE), implica ineludiblemente el tratamiento de información relativa a niños, niñas y adolescentes –muchos de ellos estudiantes en situación de vulnerabilidad- quienes merecen una protección más intensa de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de los mismos.

A este respecto, se debe tener presente que el legislador ha optado por entregar un nivel especial de protección a los datos personales que se refieren a las características físicas de las personas, como es el caso de los datos biométricos, por cuanto considera que cualquier acto de tratamiento de este tipo de datos es particularmente propenso a lesionar los derechos fundamentales de su titular, razón por la cual ha establecido que "[n]o 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 correspondan a sus titulares" (artículo 10 de la Ley N°19.628). Por otra parte, cabe mencionar que el Consejo para la Transparencia ha señalado que los datos de los menores de edad son, *per se*, datos personales sensibles y que, por lo tanto, deben ser especialmente protegidos.

En vista a lo anterior, este Consejo, en primer lugar, hace un llamado a evaluar en profundidad la necesariedad y proporcionalidad de esta clase de medidas, en vista a los objetivos que se persiguen con su implementación y los riesgos que implica el tratamiento de datos personales especialmente protegidos. Así, debe ponderarse si la finalidad de "certificar las raciones efectivamente servidas a los beneficiarios del programa PAE" no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para la intimidad de niños, niñas y adolescentes, y para su derecho a la protección de datos de carácter personal específicamente sensibles.

Si, luego de efectuado el referido balance entre los derechos y bienes jurídicos comprometidos, su institución estima que no resulta técnicamente posible implementar otras medidas de certificación que afecten en menor grado los derechos a la intimidad y protección de datos personales de niños, niñas y adolescentes, persistiendo en el empleo de herramientas biométricas, será necesario adoptar un conjunto de disposiciones organizativas, materiales y procedimentales que garanticen, en todo momento, los máximos niveles de resguardo a los beneficiarios del programa PAE. Así, resulta indispensable considerar, a lo menos, los siguientes elementos:

1. **Consentimiento.** Tratándose de datos sensibles de menores de edad, su tratamiento supone el consentimiento de quienes tengan la representación legal de los mismos, el que debe ser previo, informado, expreso, por escrito y específico, tanto respecto:
   (i) de las operaciones concretas de tratamiento que pueden ser realizadas;
   (ii) la delimitación de la finalidad o finalidades que motivan dicho tratamiento;
   (iii) la identificación precisa de los datos sensibles que serán objeto de alguna de las actividades de tratamiento antes descritas; y
   (iv) la individualización de las entidades que han sido habilitadas para ello.

   Todas estas consideraciones tienen que ser adecuadamente informadas -empleando un lenguaje claro- al momento de la recolección del consentimiento, en el respectivo formulario de registro, entregándose copia del mismo al representante legal del menor enrolado. Con todo, dicha información también debiese ser puesta a disposición permanente del público, tanto en la plataforma web de su institución como en los sitios electrónicos de los establecimientos educacionales en los cuales se recaba el referido consentimiento, a efectos de facilitar su consulta.

2. **Finalidad.** Teniendo presente la debida observancia del principio de finalidad, contenido en el inciso primero del artículo 9° de la Ley N°19.628, las operaciones de tratamiento que se realicen respecto de los datos en cuestión deberán circunscribirse estrictamente

a los objetivos definidos e informados al momento de su recolección, esto es, verificar el suministro de raciones alimenticias para los beneficiarios del PAE. Cualquier actividad de tratamiento que no se enmarque dentro de dicha finalidad sería ilícita, pudiendo originar las responsabilidades que determine la ley.

3. **Conservación y eliminación.** Los datos personales proporcionados se conservarán solo durante el tiempo necesario para cumplir con la finalidad para la que se recaban, el que en todo caso no podrá ser superior a 5 años. En la eventualidad que se requiera extender dicho plazo, se deberá obtener nuevamente el consentimiento del titular de los datos o su representante legal. Con todo, una vez transcurrido el referido plazo o cumplida la finalidad que motivó su recolección, el responsable del tratamiento debe proceder con la eliminación de todos los datos recolectados, por cuanto el almacenamiento de éstos carecería de fundamento legal. En este proceso de eliminación de los datos, se sugiere adoptar las medidas técnicas necesarias para impedir que se pueda reversar la operación y recuperar posteriormente los datos eliminados.

4. **Derechos ARCO.** El titular de los datos proporcionados o sus representantes legales, tienen derecho a ejercer en cualquier momento los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO). En este sentido, es necesario comunicar adecuadamente a los titulares o sus representantes la posibilidad de ejercer -tanto de manera presencial como remota- estos derechos, señalando los respectivos canales de contacto, lo que debe ser informado de manera clara al momento de la recolección del consentimiento, en el respectivo formulario de registro. Dicha información de contacto debe ser puesta a disposición permanente del público, tanto en la plataforma web de su institución como en los sitios electrónicos de los establecimientos educacionales en los cuales se recaba el referido consentimiento, a efectos de facilitar su consulta.

5. **Medidas de seguridad.** Conforme a las Recomendaciones del Consejo para la Transparencia sobre Protección de Datos Personales por parte de los Órganos de la Administración del Estado, se deben adoptar "todas las medidas, tanto organizativas como técnicas, para resguardar la integridad, confidencialidad y disponibilidad de los datos contenidos en sus registros con la finalidad de evitar la alteración, pérdida, transmisión y acceso no autorizado de los mismos. Para ello, los organismos públicos aplicarán diversos niveles de seguridad atendiendo al tipo de dato almacenado, a título ejemplar, respecto de los datos sensibles deberán adoptarse niveles de seguridad más altos que en relación a aquellos que no poseen dicha calidad". Así, en vista a la especial naturaleza de los datos personales que son objeto de tratamiento en el caso en comento, resulta imprescindible garantizar en todo momento la máxima seguridad de esta información, mediante el uso de sistemas informáticos actualizados y protegidos; la incorporación de procedimientos para la prevención de filtraciones y accesos indebidos; el empleo de mecanismos de encriptación para asegurar la integridad y confidencialidad de la información; y la definición de perfiles de acceso.

   Por otra parte, en el evento de sufrir ataques o intrusiones al banco de datos, resulta necesario adoptar las medidas especiales de resguardo de la información que el caso amerite, con el objeto de preservar su integridad. Asimismo, se deberá informar a los titulares de los datos o sus representantes legales de eventuales brechas de seguridad, las posibles consecuencias de estas vulneraciones y las medidas de solución o resguardo adoptadas.

6. **Confidencialidad.** En vista a lo dispuesto en el artículo 7° de la Ley N° 19.628, se recomienda establecer deberes de confidencialidad estrictos, garantizando su cumplimiento respecto de todas aquellas personas que participen en el tratamiento de los datos recolectados. En el evento que se empleen a entidades privadas para el tratamiento de datos –por ejemplo, servicios informáticos de almacenamiento o registro– se deberán establecer las obligaciones de confidencialidad en los contratos de prestación de servicios o en un anexo a los mismos, quedando claramente establecidas las responsabilidades en caso de incumplimiento a los deberes de seguridad y confidencialidad, o de infracciones a la finalidad establecida en la contratación. Esta clase de medidas permite consolidar los mecanismos de resguardo y garantizar la plena aplicación de la legislación respecto de terceros que traten datos personales.

7. **Política de privacidad.** Todos los elementos expuestos anteriormente deben constar en una política de privacidad. Así, la referida política deberá informar a los interesados, de manera completa y empleando un lenguaje claro, acerca de la entidad responsable de la base de datos personales; la finalidad de la recolección; las operaciones de tratamiento que tendrán lugar respecto de los datos; el período de conservación; su eventual tratamiento por terceros mandatarios; las medidas técnicas y organizativas que garantizan su seguridad; y los derechos que asisten a sus titulares de los datos y la forma cómo pueden ser ejercidos; entre otros elementos. Esta política de privacidad debe ser puesta a disposición permanente del público, tanto en la plataforma web de su institución como en los sitios electrónicos de los establecimientos educacionales en los cuales se recaba el referido consentimiento, a efectos de facilitar su consulta.

8. **Responsabilidad.** Finalmente, se debe tener presente que, en virtud a lo dispuesto en el artículo 11 de la Ley N° 19.628, JUNAEB, como responsable del tratamiento de los datos recolectados (y aun cuando dicho tratamiento pueda ser mandatado o encargado a un tercero) debe cuidar de ellos con la debida diligencia, haciéndose responsable de posibles daños.

Sin otro particular, le saluda atentamente

REPÚBLICA DE CHILE ★ Presidente ★ CONSEJO PARA LA TRANSPARENCIA

MARCELO DRAGO AGUIRRE
PRESIDENTE
Consejo para la Transparencia

JRY/ARR/PCV/EBP/PTR
DISTRIBUCIÓN:
- Junta Nacional de Auxilio Escolar y Becas
- Archivo