Ciudad de México, a 19 de diciembre de 2017
INAI/187/17

SRE DEBE DAR A CONOCER CONVENIOS SOBRE TRANSFERENCIAS DE DATOS PERSONALES: INAI

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) ordenó a la Secretaría de Relaciones Exteriores (SRE) entregar versiones públicas de los convenios que ha suscrito con la Secretarías de Gobernación y de Seguridad Pública (Segob y SSP), el Centro de Investigación y Seguridad Nacional (Cisen) y la Procuraduría General de la República (PGR) para la transferencia de datos personales de los ciudadanos que tramitan su pasaporte.

Un particular solicitó conocer los convenios que ha celebrado la SRE con las dependencias del gobierno Federal, con la finalidad de transmitir datos personales de los ciudadanos que tramitan su pasaporte. En respuesta, la dependencia manifestó que ha suscrito cuatro convenios con: la Segob, el Cisen, la PGR y la SSP, con el propósito de intercambiar información relacionada con la nacionalidad y naturalización, visas, pasaporte, protección consular, registro de sentenciados y procesados.

Sin embargo, precisó que los contratos se encontraban reservados por seguridad nacional, ya que su difusión pondría en riesgo los mecanismos de intercambio de información, ante lo cual el particular manifestó inconformidad, por lo que interpuso un recurso de revisión ante el INAI. En alegatos, la dependencia reiteró su respuesta.

Al presentar el caso ante el Pleno, la comisionada Areli Cano Guadiana aseguró que la transferencia de datos personales es un factor clave de colaboración entre distintas instituciones, a fin de hacer más efectiva y eficiente las labores de gestión de las responsabilidades públicas.

“En la actualidad este tipo de registros son un insumo para el análisis y la toma de decisiones en diversos ámbitos, como el de la prevención y persecución de delito, para lo cual el Estado aprovecha que sus distintos organismos recolecten este tipo de información para funciones específicas, lo que después facilita su transmisión”, explicó.

Areli Cano destacó que el nuevo marco normativo mexicano en materia de protección de datos personales, prevé mecanismos para que, en un entorno de comunicación interinstitucional, se lleven a cabo transferencias y se propicien las condiciones necesarias para garantizar a cabalidad el derecho humano de protección de datos personales.

En este contexto, se llevó a cabo el análisis del caso, del cual se advirtió que, si bien los convenios referidos se celebran en el marco de actividades de coordinación con instituciones responsables de la Seguridad Nacional, contienen ciertos rubros de carácter general que no pueden reservarse.

Derivado de una diligencia de acceso a la información clasificada, se verificó que dichos rubros contienen sólo las condiciones y términos pactados para cumplir con los fines de los convenios, aspectos de naturaleza pública, que documentan la gestión del sujeto obligado en la ejecución de las atribuciones conferidas y el ejercicio de recursos públicos, es decir, la información no se relaciona con las estrategias de inteligencia que pudiese representar una amenaza para el país.

No obstante, se comprobó que los detalles de los sistemas informáticos implementados para la transferencia de los datos y las especificaciones tecnológicas para la consulta de los registros sí es procedente, pues al darlos a conocer se difundirían especificaciones útiles para la generación de Inteligencia, además de que esos elementos constituyen mecanismos y metodologías que permitirían el acceso no autorizado a los registros, lo cual afectaría la eficacia de las acciones de salvaguarda de la Nación.

Adicionalmente, en la diligencia de acceso, se observó que los convenios contienen también los nombres y firmas de los servidores públicos adscritos a las instituciones firmantes. Al respecto, se puntualizó que, por regla general, los nombres de los funcionarios son de carácter público, salvo de aquellos implicados en actividades operativas de Seguridad. En ese sentido, se concluyó que la dependencia debe proteger la información del personal del Cisen y de las otras dependencias involucradas, siempre y cuando desempeñe funciones operativas.

Lo anterior, en razón de que, al dar a conocer sus nombres, podrían ser identificados y estar expuestos a amenazas por parte de la delincuencia organizada, con el fin de obtener los pormenores para acceder a los mecanismos de intercambios de comunicación, con lo cual se vulnerarían no sólo sus actividades sino su vida, salud e integridad física e, incluso, la de su entorno familiar.

“La resolución propuesta determina la entrega de la información que da pauta para que la sociedad se entere de los pormenores de la actuación institucional en el manejo de datos entregados para el trámite de los documentos de viaje, al tiempo que se asegura que no se lesionan otros intereses jurídicamente tutelados como en este caso el de la seguridad nacional”, subrayó la comisionada Cano Guadiana.

Por lo expuesto, el Pleno del INAI determinó modificar la respuesta de la SRE, a fin de que entregue al particular versiones públicas de los convenios y sus anexos, en los que únicamente podrá clasificar por seguridad nacional el detalle de los sistemas, equipos o base de datos y las especificaciones técnicas para la transferencia de información, así como el nombre y firma de los servidores públicos del Cisen y de aquellos con funciones operativas de las demás dependencias.

-o0o-

Comisionada ponente: Areli Cano Guadiana
Sujeto obligado: Secretaría de Relaciones Exteriores
Folio: 0000500181817
Expediente: RRA 6596/17