

TRANSFERENCIA Y SEGURIDAD DE DATOS REGISTRALES

*Silvia Susana Toscano*¹

RESUMEN:

La transferencia de los datos correspondientes a las sociedades cobra una relevancia al tenor de las nuevas tecnologías de almacenamiento en la nube que, en la mayoría de los casos, se verifica como un flujo de datos transfronterizo. Se pretende analizar la aplicación de las normas generales que rigen en la Ley de Protección de Datos personales respecto de la transferencia internacional, así como relevar las normas de seguridad que deberán tenerse en cuenta para salvaguardar la protección de los datos registrales y otros de las sociedades que se encuentran bajo control de la Inspección General de Justicia (IGJ). Se estructura de la siguiente manera:

Título: Transferencia y seguridad de datos registrales

1. Introducción
2. Transferencia Internacional de Datos Personales
3. Normas corporativas vinculantes (NCV)
4. Conclusiones



1. Introducción

Tanto las personas humanas como las jurídicas generan un volumen cada vez mayor de información a nivel mundial. Se estima que en 2025, este volumen ascenderá a un total de 163 zettabyte, 10 veces más que el volumen actual².

¹ Con colaboración de Virginia Scharn (Docente e Investigadora en la Universidad Argentina de la Empresa -UADE)

² Fuente: Data Age 2025, IDC www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf

El incremento en la recolección de datos con diversos objetivos y la magnitud del intercambio sumado al almacenamiento de los mismos en la nube supone un escenario donde se hace imprescindible la adopción de medidas de seguridad y confidencialidad que generen confianza en los usuarios del ciberespacio para el desarrollo económico.

Frente a este escenario, se hace imprescindible que las empresas adopten normativas internas tendientes a otorgar una adecuada protección a los datos personales y toda otra información que recopilan, almacenan y tratan y el Estado deberá prever estos adelantos tecnológicos a efectos de darles el marco normativo adecuado.

Con ese objetivo, la Unión Europea decidió establecer un marco más sólido y coherente en materia de protección de datos en la UE, con una aplicación estricta que permitiera el desarrollo de la economía digital en el mercado interior, otorgue a los ciudadanos el control de sus propios datos y refuerce la seguridad jurídica y práctica de los operadores económicos y las autoridades públicas.

La puesta en vigencia en mayo de 2018 del Reglamento General de Protección de Datos de la Unión Europea, en adelante DGPR, ha significado cambios sustanciales en la forma de tratamiento y difusión de los datos personales recabados por el Estado y los privados. Asimismo, esta normativa resulta de aplicación no sólo para las sociedades comerciales que se encuentren radicadas en el territorio de la UE sino también todas aquellas que ofrecen servicios y productos a residentes en los países de la UE.

2. Transferencia Internacional de Datos Personales

Es preciso recordar la regulación que obra en la ley argentina de Protección de Datos Personales -Ley 25.326- sobre la transferencia internacional de datos personales. El artículo 12 de dicha ley establece que la misma se encuentra permitida siempre y cuando el país destinatario de la información proporcione niveles de protección adecuados³. No se precisa en el articulado cuáles son los criterios que se adoptan en dicha consideración.

³ *Artículo 12.-* (Transferencia internacional).

1. Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados.
2. La prohibición no regirá en los siguientes supuestos:
 - a) Colaboración judicial internacional;

Para ahondar en el concepto de “niveles de protección adecuados”, es preciso remitirse al Decreto Reglamentario de la Ley 25.326 (Decreto 1558/01)

“El carácter adecuado del nivel de protección que ofrece un país u organismo internacional se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración de tratamiento o de los tratamientos previstos, el lugar de destino final, las normas de derecho, generales o sectoriales, vigentes en el país de que se trate, así como las normas profesionales, códigos de conducta y las medidas de seguridad en vigor en dichos lugares, o que resulten aplicables a los organismos internacionales o supranacionales”.

En definitiva, se entiende que un Estado u organismo internacional proporciona un nivel adecuado de protección cuando dicha tutela se deriva directamente del ordenamiento jurídico vigente, o de sistemas de autorregulación, o del amparo que establezcan las cláusulas contractuales que prevean la protección de datos personales.

Dice el informe de la comisión redactora del nuevo reglamento de la Unión Europea en lo relativo a la transferencia internacional de datos personales entre privados o entre estados. “... El carácter adecuado del nivel de protección que ofrece un país u organismo internacional se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración de tratamiento o de los tratamientos previstos, el lugar de destino final, las normas de derecho, generales o sectoriales, vigentes en el país de que se trate, así como las normas profesionales, códigos de conducta y las medidas de seguridad en vigor en dichos lugares, o que resulten aplicables a los organismos internacionales o supranacionales”⁴.

En 2003, nuestro país fue considerado por la Comisión Europea con niveles adecuados de protección teniendo en cuenta la existencia de un Estado de Derecho, de herramientas jurisdiccionales y de un marco normativo con garantías acordes a las buenas prácticas en la materia Sin embargo, con la puesta en vigen-

b) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica, en tanto se realice en los términos del inciso e) del artículo anterior;

c) Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable;

d) Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte;

⁴ <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF>.

cia en 2018 del nuevo reglamento, indica que en un futuro próximo Argentina deberá re- acreditar acondicionando su legislación y las normas internas de sus empresas a los nuevos estándares de protección de datos.

3. Normas corporativas vinculantes (NCV)

En un paso significativo hacia la mencionada adecuación , la Agencia de Acceso a la Información Pública a través de la Resolución N° 159/2018, publicada el 7 de diciembre de 2018 en el Boletín Oficial aprobó los lineamientos y contenidos básicos para normas corporativas vinculantes (“NCV”), las que podrán ser utilizadas por sociedades multinacionales para la transferencia internacional de datos personales obrantes en sus registros hacia empresas integrantes del mismo grupo empresario con sede en la UE.

Estas normas son buenas prácticas y políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro de la UE para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad y viceversa.

Dicha resolución establece que las NCV extiende la obligatoriedad a sus empleados, subcontratantes y terceros beneficiarios juntamente con la aplicación de los principios rectores en materia de protección de datos personales como son la recolección lícita de los datos, la calidad de los mismos, la seguridad y la confidencialidad, la auditabilidad, entre otros.

4. Conclusiones

Como se mencionó anteriormente, el dictado del decreto que reglamenta el diseño de documentos relativos a normas de autorregulación en empresas que conformen un mismo grupo económico para la transferencia internacional de datos personales, que establece un contenido mínimo para dichas normas corporativas vinculantes significa un importante avance, ya que permitirá el intercambio de datos personales entre compañías de un mismo grupo económico sin vulnerar la normativa de protección de los mismos.

Asimismo, constituye un paso para la adecuación de las empresas argentinas al nuevo reglamento de la UE a efectos de ser competitivas en dicho mercado y, más aún, en el global.

Sin lugar a dudas, la asignación de recursos para el tratamiento de datos personales es una inversión que genera confianza y seguridad, que redundará

en un incremento de valor y ubicará a las empresas en mejores posiciones de competitividad en los mercados en que actúen.

Se ha iniciado un largo camino por recorrer; en el que el Estado tiene un rol fundamental en la adopción de tecnologías que permitan la simplificación de trámites y el acceso remoto a la información, brindando garantías de seguridad; asimismo, es esencial su intervención para dotar a estos nuevos escenarios de la regulación apropiada a fin de lograr un mayor desarrollo económico en un marco de respeto por los derechos fundamentales de los ciudadanos, entre ellos, el acceso a la información y la protección de los datos personales.