# Regulación de la transferencia internacional de datos personales en Latinoamérica. Especial mención al marco regulatorio de Argentina y México

**Christian Alejandro Razza Sandoval**
*Abogado de los Tribunales y Juzgados de la República por la Universidad de las Américas sede Quito, Ecuador*

## Resumen

**PALABRAS CLAVES:**
Dato Personal, Protección de Datos Personales, Transferencia Internacional de Datos Personales, Redes Sociales, Estándar de Protección

Los datos personales se han vuelto a nivel internacional un activo intangible que permite la productividad y competitividad. Razón por la cual se ha visto necesario regular adecuadamente su tratamiento por una serie de mecanismos, derechos y principios que garanticen el derecho a la protección de datos personales. En la actualidad este derecho se lo concibe como un derecho autónomo, complejo e instrumental. En Latinoamérica se ha marcado la tendencia de reconocer este derecho constitucionalmente, sin embargo, hasta ahora no se ha brindado las garantías suficientes para efectivizar su protección, especialmente en la transferencia internacional de datos personales (TIDP).

## Introducción

La época actual se caracteriza por una actividad social, cultural, económica, jurídica y política que constantemente rebasa fronteras. Los avances tecnológicos se han fundido con nuestro diario vivir y prácticamente todas las áreas de nuestra sociedad se ven afectadas por la tecnología. El avance tecnológico ha permitido que el tráfico de información se realice rápidamente y en grandes cantidades, lo cual, en ocasiones, se constituye como una herramienta para facilitar el desarrollo de las sociedades, y otras veces, un riesgo para los derechos de las personas (Rebollo y Serrano, 2017, pp. 21-23).

Históricamente algunas legislaciones han mostrado una preocupación mayor por la protección de datos personales, como es el caso de la Unión Europea (UE) que, en el 2016, con el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) estableció un conjunto de mecanismos para regular el tratamiento de datos personales (TOP) y la TIDP. Siguiendo esta línea, con el presente trabajo se pretende mostrar que en Latinoamérica no existe una adecuada regulación respecto a la TIDP, por lo cual si los datos personales de una persona son objeto de una de estas transferencias se encontrarían en un total estado de desprotección.

## 1. Estándares de protección para la transferencia internacional de datos personales

Por las disparidades existentes entre las legislaciones nacionales sobre protección de datos la TIDP puede poner en riesgo los derechos de las personas. Sin embargo, como señala Castellanos (2017, p. 6) sin la TIDP difícilmente se podría dar el comercio mundial. Así pues, para evitar los posibles perjuicios que a la privacidad de las personas podría causar una TIDP y poder garantizar la libre circulación de datos personales, los Estados, así como las Uniones geopolíticas (UE) han establecido estándares de protección o convenios para regular la TIDP.

En Estados Unidos el derecho a la protección de datos personales tiene como antecedente principal, el derecho a la privacidad o Right to Privacy. Esta doctrina construida por Louis Brandeis y Samuel Warren en 1890 aportó con una reinterpretación de los precedentes en la materia ya que comenzó a proteger a la privacidad fuera del derecho a la propiedad. No obstante, el sistema de protección de datos norteamericano “no reconoce la protección de la privacidad mediante una legislación específica, sino que ello se efectúa a través de normativas sectoriales que, mediante la complementación de reglamentaciones y códigos de adhesión, propician un marco regulador singular” (Castellanos, 2017, p. 14).

En Estados Unidos en el siglo XX se dictaron tres leyes que establecen los principios rectores que configuran el derecho a la privacidad en este país: la Fredoom of Information Act (FOIA) de 1966, la Privacy Act de 1974 y la Right to Financia/Privacy Act(RFPA) de 1978. En el siglo XXI aparecieron el Safe Harbar de 2000 y posteriormente el Privacy Shield de 2016 para regular la TIDP con Europa, la California Consumer Privacy Act (CCPA) de 2018 que entrará en vigor en 2020.

### Del Safe Harbour al Privacy Shield

Tanto el Safe Harbour como el Privacy Shield se concibieron como mecanismos para solucionar la ausencia de regulación en Estados Unidos sobre el TOP y permitir la TIDP con la UE. Estos marcos regulatorios son su estándar de protección para realizar la TIDP con la UE. No obstante, el Safe Harbourque fue el marco regulatorio que más tiempo estuvo vigente, aunque fue acogido por miles de empresa americanas, no era de carácter obligatorio, no estaba en igual rango que otras leyes americanas y se encontraba desactualizado, lo cual dificultaba su aplicación y, por ende, tuvo que ser sustituido. El Privacy Shield si bien entró a cubrir los vacíos de su antecesor sigue cayendo en los mismos problemas, no es un marco regulatorio obligatorio y no implica que Estados Unidos sea un país con un nivel adecuado de protección de datos personales.

La regulación sobre protección de datos personales en la UE ha venido desarrollándose a lo largo del tiempo con gran interés debido a que, por la evolución de las tecnologías de la información y comunicación (TICs) se ha podido realizar un intercambio inmediato de informa-

ción sin límites físicos. En la UE desde el Convenio 108 de 1981 se ha emitido varias normas comunitarias que regulan la protección de datos personales, requiriendo una "protección equivalente" entre los países partes, y buscando una cooperación internacional a través de las autoridades locales de cada país.

Una de las normativas más importantes fue la Directiva 95/46/CE, del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al TDP y a la libre circulación de estos datos. Los Estados miembros de la UE, a efectos de cumplir con las obligaciones que imponía este Directiva, fueron elevando progresivamente el nivel de protección de los datos personales, produciéndose "un efecto homogeneizador de los medios de protección y de los mecanismos para la eficacia de los derechos" (Rebollo, 2008, p. 105). Como resultado de este proceso, con la expedición del GDPR la normativa de la UE en el campo de la protección de los datos se ha constituido como la más exigente del planeta (Guasch, 2012, p. 22).

### Reglamento General de Protección de Datos

En Europa el 27 de abril de 2016 se adoptó el Reglamento (UE) 2016/679 del Parlamento y del Consejo, con el que se derogó la Directiva 95/46/CE a fin de reformar la normativa ya existente sobre protección de datos personales y adaptarla al nuevo contexto mundial que después del caso de Cambridge Analytica cambió notablemente. Con el GDPR la UE estableció todo un sistema de protección de datos personales, que modificó reglas ya existentes, desarrolló aquellas que eran muy básicas y creó otras que eran necesarias. Esta novedad se orienta a una transición hacia una economía centralizada en los datos y la creación de un mercado único digital (Moritz y Gibello, 2017, p. 116).

Respecto a la TIDP con el GDPR en la UE se estableció un conjunto de mecanismos para transferir datos a terceros países: decisiones de adecuación, normas contractuales estándar, normas corporativas vinculantes, mecanismos de certificación y códigos de conducta. En la UE con el GDPR para realizar una TIDP se requiere un nivel adecuado de protección. Razón por la que Estados Unidos debió implementar el Privacy Shield, y Latinoamérica se encuentra en proceso de adopción y aplicación de estándares internacionales para la protección de datos personales.

En el GDPR existen 3 niveles de protección a efectos de autorizar una TIDP a un tercer país u organización internacional. La regla general es cumplir con un nivel adecuado de protección, que es el nivel más riguroso, después viene el nivel de ofrecer garantías adecuadas; y el establecimiento de normas corporativas vinculantes o certificaciones. Además, existen casos excepcionales para realizar una TIDP.

## 2. Regulación de la protección de datos personales en América Latina

En América Latina la regulación del derecho a la protección de datos personales sigue un ritmo propio y tiene ciertas características que ameritan analizarse. Recientemente en las constituciones latinoamericanas se incorporó como derecho autónomo a la protección de datos personales frente a la necesidad de dar respuesta al proceso de evolución tecnológica (Ordóñez, 2017, p. 85).

### República de Argentina

En el Art. 43 de la Constitución de la República de Argentina se encuentra consagrado el derecho a la protección de datos personales. En este artículo se deriva la obligación de los organismos públicos de garantizar el acceso a la información, confidencialidad, supresión y rectificación de los datos personales. Pero, es en la Ley 25.336 promulgada el 4 de octubre del año 2000 donde se encuentra reglamentada la protección de datos personales. En el Art. 2 de la mencionada Ley se regula la protección de datos personales sin hacer una distinción entre el ámbito público y privado.

En el capítulo 2 de la Ley 25.326 se establece los principios generales en materia de protección de datos personales y TOP. Destacándose, el principio de licitud para la formación de archivos de datos. El principio de calidad de datos que se traduce en que la recolección

de datos no puede hacerse por medios desleales y que dichos datos deben ser ciertos y exactos, y su almacenamiento debe permitir el derecho de acceso a su titular.

En Argentina conforme el Art. 29 el órgano de control que gozará de autonomía funcional y actuará como órgano descentralizado en el ámbito del ministerio de justicia y Derechos Humanos de la Nación es la Agencia de Acceso a la Información Pública, la cual es la encargada de supervisar que se cumplan las disposiciones contenidas en la Ley 25.326. Respecto a la TIDP se sigue el modelo europeo toda vez que en el Art. 12 se exige para autorizar una TIDP que el Estado receptor de los datos cuente con un nivel adecuado de protección.

### Estados Unidos Mexicanos

El caso mexicano es particular, recién con las reformas constitucionales del año 2007 y 2009 es que se protege constitucionalmente a los datos personales, se consagra explícitamente el derecho a la protección de los datos personales y se establecen los derechos ARCO como núcleo fundamental de dicho derecho (Cunha, 2011, p.323). Posteriormente, en el año 2010 se adopta la Ley Federal de Protección de Datos en Posesión de Particulares, teniendo un ámbito de aplicación únicamente privado. Dada la redacción de esta Ley es evidente que se basa en el marco normativo europeo apuntando hacia la tendencia mundial de regulación jurídica de los datos personales para garantizar el derecho a la vida privada de los individuos, con respecto al TOP.

En la mencionada Ley se establece una serie de principios para la protección de datos personales, como son: el de información, licitud, consentimiento, calidad, finalidad, lealtad, proporcionalidad y responsabilidad. En el capítulo VI establece las competencias de la Autoridad reguladora, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). En capítulo V se desarrolla la TIDP, pero, no se exige un nivel adecuado de protección, tan solo exige consentimiento del titular de los datos y enumera ciertos supuestos que no requieren consentimiento, además no desarrolla las transferencias ulteriores.

El 26 de enero de 2017, se expidió la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados con el fin de regular el ámbito público del TDP. Son sujetos obligados conforme el Art. 1 en el ámbito federal, estatal y municipal: “cualquier autoridad, entidad, órgano y organismo de los poderes ejecutivo, legislativo y judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.”. Los particulares, sean personas naturales o jurídicas, no le son aplicables esta Ley sino la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

En el capítulo 1 del Título segundo de la Ley aplicable a sujetos obligados, en relación con la Ley aplicable a privados se aumenta y se desarrolla un conjunto de principios que el responsable del tratamiento debe cumplir cuando recolecta, almacena, usa, circula o realiza cualquier actividad con datos personales, como son los: principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad demostrada en el TOP. De la autoridad de protección de datos personales señala que sigue siendo el INAI. En lo que se refiere a la TIDP en el Art. 68 de la Ley aplicable a los sujetos obligados se señala que:

> *“El responsable sólo podrá transferir o hacer remisión de datos personales fuera del territorio nacional cuando el tercero receptor o el encargado se obliguen a proteger los datos personales conforme a los principios y deberes que establece la presente Ley.”*

De esta norma se evidencia que para autorizar una TIDP se exige el cumplimiento de garantías adecuadas, además de necesitar el responsable del TDP el consentimiento del titular de los datos y deberá comunicar al receptor de los datos personales las finalidades conforme a las cuales se tratan los datos personales frente al titular. No obstante, no se requiere un nivel adecuado de protección como en la UE con el GDPR.

## Comparación entre las regulaciones

Del estudio realizado se evidenció que el derecho a la protección de datos personales se tutela de una manera diferente a nivel mundial, aunque con una tendencia a dirigirse al modelo europeo. Además, debido a los riesgos de la TIDP, se ha marcado una predisposición de los Estados y las organizaciones internacionales de exigir un nivel adecuado de protección de datos personales para autorizar una TIDP. Así pues, a partir del análisis realizado sobre la regulación de la protección de datos personales, corresponde efectuar una comparación centrada en los temas que son objeto de este trabajo.

***Tabla 1. Comparación con respecto a la protección de datos personales***

| | Latinoamérica | | Europa | | |
|---|---|---|---|---|---|
| | **Argetnitna** | **México** | **GDPR** | **EE.UU.** | **OCDE** |
| Norma constitucional sobre la protección de datos | • | • | NA | X | NA |
| Legislación general sobre protección de datos personales | • | • | • | X | • |
| Normativa sectorial en cuanto al TDP | • | • | NA | • | NA |
| TDP especial para datos personales sensibles | • | • | • | X | • |
| Autoridad autónoma competente | • | • | • | X | • |
| Recursos administrativos y acciones judiciales | • | • | • | • | • |
| Obligaciones a los responsables y encargados de los TDP | • | • | • | X | • |
| Principios para el TDP y la TIDP | • | • | • | X | • |
| Derechos ARCO | • | • | • | X | • |
| Sanciones | • | • | • | • | • |
| Regulación sobre la TIDP | • | • | • | • | • |

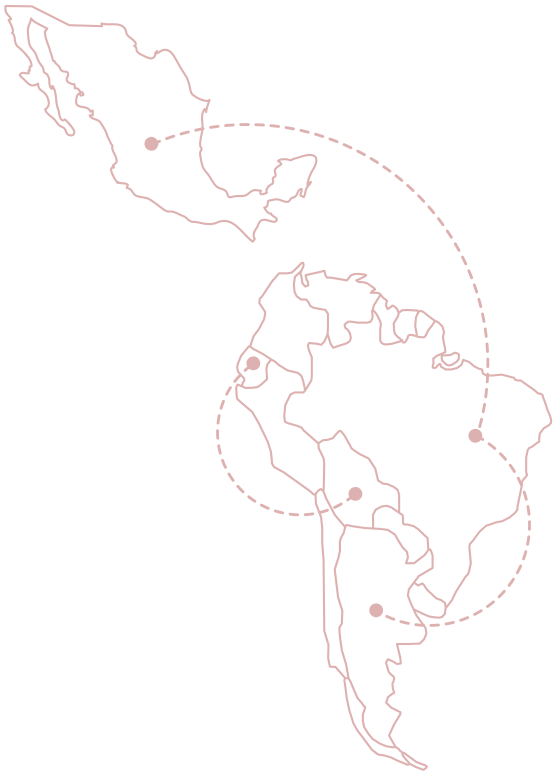
*Nota: NA - no aplica*

***Tabla 2. Comparación general respecto a la TIDP***

| | **Argentina** | **México** | **GDPR** | **Privacy Shield** | **OCDE** |
|---|---|---|---|---|---|
| Definición sobre la TIDP | X | X | X | X | X |
| Desarrollo de las TIDP ulteriores | X | X | • | • | • |
| Exigencia de un nivel adecuado para la TIDP | • | X | • | • | • |
| Garantías adecuadas para la TIDP | X | • | • | X | • |
| Normas corporativas vinculantes para la TIDP | X | • | • | • | • |
| Casos excepcionales para la TIDP | • | • | • | • | • |

*Nota: Comparación de los niveles de protección para realizar una TIDP.*

Como se puede notar Estados Unidos con el Privacy Shield, Latinoamérica y los organismos internacionales se alinean al estándar de protección de datos personales que establece la UE con el GDPR. Se resalta la necesidad de contar con autoridades de control autónomas como la AEPD en España o la CNIL en Francia para un correcto desarrollo de la protección de datos. En cuanto a la TIDP de igual manera se sigue la tendencia europea de establecer niveles de protección adecuados que permitan proteger a los titulares de los datos.



## Conclusiones

Desde la incorporación y posterior desarrollo de las nuevas tecnologías, Latinoamérica ha pasado por una revolución en el manejo de la información. La combinación de estas herramientas tecnológicas con el fenómeno de la globalización trajo consigo múltiples ventajas, como: el desarrollo del comercio electrónico, la implementación de un gobierno en línea, y la virtualización de las relaciones de los ciudadanos, proveedores, consumidores y autoridades. Todas estas actividades requieren de la TIDP, por ello la necesidad de buscar armonizar las legislaciones en cuanto a la protección de datos personales.

En Latinoamérica, si bien son varios los países que regulan la protección de datos personales para proteger los derechos de sus ciudadanos, y desarrollar el comercio internacional y electrónico, aun existen ciertas falencias en la regulación. Por ejemplo, contar con una autoridad de control independiente, regular adecuadamente la TIDP, poder sancionar a los infractores con multas que puedan causar un grado de responsabilidad y actualizar las legislaciones sobre protección de datos. Falta todavía mucho para lograr la protección que brinda el GDPR, pero un paso importante es comenzar a tener una cultura de protección de nuestros datos personales.

## Referencias bibliográficas


Castellanos, A. (2017). El régimen jurídico de las transferencias internacionales de datos personales. Especial mención al marco regulatorio Privacy Shield. /CPS Working Papers, 350. Recuperado el 15 de octubre de 2019 de https://www.icps.cat/archivos/Workingpapers/wp350.pdf?noga=1

Cunha, T. D. (2011). Las recientes reformas en materia de protección de datos personales en México. Anuario Jurídico y Económico Escurialense. Recuperado el 29 de octubre de 2019 de https://webcache.googleusercontent.com/search?q=cache:QvlznE2P Z80J:https://dialnet.unirioja.es/descarga/articulo/3625376.pdf+&cd=1&hl=es&ct=clnk&gl=ec

Eur-Lex. (s.f.). Decisión de ejecución, Privacy Shield UE-EE. UU 201611250de Ja Comisión Europea de 12 de julio de 2016. Recuperado el 2 de septiembre de 2019 de https://eur-lex.europa.eu/legal- content/ES/TXT/PDF/?uri=CELEX:320 1601250&qid=154266055680 3&from=EN

Eur-Lex. (s.f.). Decisión de Ja Comisión 20001520/CE, Safe Harbar Privacy Principies de la Comisión Europea de 26 de julio de 2000. Recuperado el 2 de octubre de 2019 de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32000D0520&from=en

Eur-Lex. (s.f.). Reglamento General de Protección de datos del Parlamento Europeo y del Consejo UE 20161679(GDPR) de 2016. Recuperado el 15 de octubre de 2019 de https://eur-lex.europa.eu/legal- content/ES/TXT/PDF/?uri=CELEX:320 16R0679&from=ES

Gibello, V. y Moritz, M. (2017). El Reglamento Europeo (UE) 2016/679: análisis de un claroscuro. Foro, 27. Recuperado el 25 de octubre de 2019 de http://repositorio.uasb.edu.ec/bitstream/10644/5948/1/08-TC-Moritz- Gibello.pdf

Guasch Portas, V. (2012). La transferencia internacional de datos de carácter personal. RDUNED, 11. Recuperado el 20 de octubre de 2019 de http://revistas.uned.es/index.php / RDUNED/article/view/11139/10667

Honorable Cámara de Diputados. (s.f.). Ley Federal de Protección de Datos Personales en Posesión de /os Particulares de México de 2010. Recuperado el 30 de septiembre de 2019 de http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Honorable Cámara de Diputados. (s.f.). Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados de México de 2017. Recuperado el 14 de septiembre de 2019 de http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

Ordóñez, L. (2017). La protección de datos personales en los estados que conforman la Comunidad Andina: estudio comparado y precisiones para un modelo interamericano de integración. Foro, 27. Recuperado el 14 de octubre de 2019 de http://repositorio.uasb.edu.ec/bitstream/10644/5947/1 /07-TC- Ordo%C3%B 1 ez.pdf

Organización de Estados Americanos. (s.f.). Ley de Protección de Datos Personales de Argentina, Nro. 25.326 de 2000. Recuperado el 25 de septiembre de 2019 de https://www.oas.org/juridico/PDFs/arg_ley25326.pdf

Rebollo, L. (2008). Vida privada y protección de datos en la Unión Europea. Madrid: Dykinson.

Rebollo, L. y Serrano, M. M. (2017). Manual de Protección de Datos (2a. ed.). Madrid: Dykinson.

Zaballos, E. (2013). La Protección de Datos Personales en España: Evolución Normativa y Criterios de Aplicación (Tesis Doctoral). Recuperado el 18 de octubre de 2019 de https://eprints.ucm.es/22849/1/T34733.pdf



### Christian Alejandro Razza Sandoval

Abogado de los Tribunales y Juzgados de la República por la Universidad de las Américas sede Quito, Ecuador. Experiencia laboral en el ámbito público como privado en temas laborales, societarios y de niñez y familia. Actualmente es asesor legal del Hospital Vozandes en el área de propiedad intelectual y Abogado Jr. En Fabara &Compañía Abogados en el área laboral y de telecomunicaciones. Ha participado en varios proyectos de vinculación con la comunidad, como combatir la violencia intrafamiliar, también participo en la creación de una ley de protección de datos personales para el Ecuador.