UNIVERSIDAD SAN FRANCISCO DE QUITO USFQ

Colegio de Jurisprudencia

El régimen de transferencia internacional de datos personales. Un enfoque en la autorregulación

Fátima Carolina Llumiluisa Falconí

Jurisprudencia

Trabajo de fin de carrera presentado como requisito para la obtención del título de Abogada

Quito, 20 de noviembre de 2022

© DERECHOS DE AUTOR

Por medio del presente documento certifico que he leído todas las Políticas y Manuales de la Universidad San Francisco de Quito USFQ, incluyendo la Política de Propiedad Intelectual USFQ, y estoy de acuerdo con su contenido, por lo que los derechos de propiedad intelectual del presente trabajo quedan sujetos a lo dispuesto en esas Políticas.

Asimismo, autorizo a la USFQ para que realice la digitalización y publicación de este trabajo en el repositorio virtual, de conformidad a lo dispuesto en la Ley Orgánica de Educación Superior del Ecuador.

Nombres y apellidos:	Fátima Carolina Llumiluisa Falconí
Código:	00202900
Cédula de identidad:	1721638250
Lugar y Fecha:	Quito, 20 de noviembre de 2022.

ACLARACIÓN PARA PUBLICACIÓN

Nota: El presente trabajo, en su totalidad o cualquiera de sus partes, no debe ser considerado como una publicación, incluso a pesar de estar disponible sin restricciones a través de un repositorio institucional. Esta declaración se alinea con las prácticas y recomendaciones presentadas por el Committee on Publication Ethics descritas por Barbour et al. (2017) Discussion document on best practice for issues around theses publishing, disponible en http://bit.ly/COPETheses.

UNPUBLISHED DOCUMENT

Note: The followuing capstone Project is available through Universidad San Francisco de Quito USFQ institutional repository. This statement follows the recommendations presented by the Committee on Publication Ethics COPE described by Barbour et al. (2017) Discussion document on best practice for issues around theses publishing available on http://bit.ly/COPETheses.

EL RÉGIMEN DE TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES. UN ENFOQUE EN LA AUTORREGULACIÓN[1]

THE INTERNATIONAL TRANSFER REGIME OF PERSONAL DATA. A FOCUS ON SELF-REGULATION

Fátima Carolina Llumiluisa Falconí[2]
faticaro4@hotmail.com

RESUMEN

El constante intercambio de información en las relaciones comerciales del mundo obliga a que los países observen estándares de protección en la transferencia internacional de datos personales. Este trabajo identificó las principales falencias en la legislación del Ecuador, que no cuenta con un nivel adecuado de protección. Con la aplicación de un método deductivo y comparativo entre el sistema europeo y el nacional, se presentó a la autorregulación como respuesta al sector empresarial para enfrentar dicho problema. Mediante la aplicación de normas corporativas vinculantes y códigos de conducta, se puede observar el cumplimiento del principio de responsabilidad proactiva, que es parte de la columna vertebral del sistema de protección de datos personales.

PALABRAS CLAVE

Principio de responsabilidad proactiva, normas corporativas vinculantes, protección de datos, transferencia internacional de datos personales, bancos de datos.

ABSTRACT

The constant exchange of information in world trade relations forces countries to observe protection standards in the international transfer of personal data. This work identified the main shortcomings in the Ecuadorian legislation, which does not have an adequate level of protection. With the application of a deductive and comparative method between the European and the national system, self-regulation was presented as a response to the business sector in order to face this problem. Through the application of binding corporate rules and codes of conduct, compliance with the accountability principle can be observed, which is part of the backbone of the personal data protection system.

KEY WORDS

Accountability principle, binding corporate rules, data protection, international transfer of personal data, data bank.

Fecha de lectura: 20 de noviembre de 2022

Fecha de publicación: 20 de noviembre de 2022

[1] Trabajo de titulación presentado como requisito para la obtención del título de Abogada. Colegio de Jurisprudencia de la Universidad San Francisco de Quito. Dirigido por el Dr. Felipe Francisco Coronel Carcelén.

SUMARIO:

1. Introducción

El número de transacciones comerciales a nivel internacional ha ido aumentando durante los últimos años en un escenario de globalización y desarrollo tecnológico. En cada transacción, millones de datos de carácter personal viajan desde y hacia diferentes partes del mundo. Por lo tanto, están constantemente expuestos a ser utilizados para fines distintos a los que en un inicio fueron autorizados, y sin la debida autorización de sus titulares. Esto es peligroso porque los datos personales se han convertido en activos intangibles de alto valor y el mundo ha visto las consecuencias de su tratamiento inadecuado, como por ejemplo en el caso de *Cambridge Analytica*[3].

Ante este problema, la mayoría de las legislaciones se han comprometido en proteger el tratamiento de datos personales. A nivel internacional, el sistema jurídico que lidera en materia de protección de datos es el europeo. A partir de ese modelo, Ecuador promulgó el 26 de mayo de 2021 la Ley Orgánica de Protección de Datos Personales, LOPDP, cuyo régimen sancionatorio está pronto a entrar en vigencia[4].

La adopción de una ley de rango orgánico supone un gran paso para el país. Sin embargo, las máximas que han sido desarrolladas por un sistema tan evolucionado como el europeo, están mucho menos avanzadas en el escenario nacional, especialmente, en el cumplimiento de los estándares de transferencia internacional de datos. El Ecuador no llega al nivel de protección adecuado que el régimen europeo demanda, para ser catalogado como un destino seguro de intercambio de datos. Además, el reglamento a la LOPDP y la Superintendencia de Protección de Datos aún están en proceso de creación.

[3] Se trata del escándalo en que esta empresa inglesa se vio sumergida por diseñar campañas políticas orientadas a influir en el comportamiento de los votantes en las elecciones presidenciales de Estados Unidos de 2016, con base en los perfiles psicológicos construidos a partir de datos recabados de Facebook, sin autorización de los usuarios.

[4] El régimen sancionador empezará a regir desde el 26 de mayo de 2023.

Al no ser considerado como país seguro de intercambio de información, el sector empresarial se quedaría fuera de vista de potenciales alianzas internacionales para celebrar acuerdos comerciales que involucren el tratamiento y trasferencia de datos. Eso acarrea una gran desventaja económica, sobre todo, porque la economía se mueve, cada vez más, en el plano digital.

Dadas estas consideraciones, ¿cómo puede el sector empresarial ecuatoriano ponerse al nivel internacional en la transferencia de datos personales para ser considerado como destino seguro de intercambio?, y ¿qué mecanismos tienen las empresas para demostrar compromiso en el cumplimiento a la normativa y adhesión a una cultura de ética corporativa?

Para abordar dichas preguntas, este trabajo propone, primero, comparar los estándares europeos con los que establece la LOPDP sobre transferencia internacional de datos personales, señalando las falencias en la legislación local. Luego, detallar el alcance de la responsabilidad proactiva y demostrada como principio transversal del sistema de protección de datos y su relación con la autorregulación empresarial. Después, analizar las normas corporativas vinculantes y códigos de conducta como herramientas clave en la adecuación de los estándares europeos. Finalmente, hacer énfasis en el fortalecimiento de la cultura ética y responsabilidad social corporativa.

2. Estado de la cuestión

El derecho de protección de datos personales no fue siempre considerado como fundamental, autónomo e independiente. De hecho, es una derivación del derecho a la privacidad, mismo que, a palabras de Aristeo García, protege la promoción de la libertad individual[5]. Al respecto, García destaca la obra de J. Stuart Mill, *On Liberty*, en las que se relaciona a la libertad con la independencia privada[6].

No es sino con la publicación de la obra *The Right to Privacy* en 1890, escrita por los juristas Samuel Warren y Louis Brandeis en Estados Unidos, con la que se sentaron las bases del derecho a la privacidad, como hoy en día se lo conoce[7]. Jonathan López-Torres explica que, en dicha obra, los autores muestran el antagonismo entre la

[5] Aristeo García González, "La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado.", *Boletín Mexicano de Derecho Comparado* 40, núm. 120 (2007), 743–78, https://doi.org/10.22201/iij.24484873e.2007.120.3933.
[6] Ibidem.
[7] Concepción Conde Ortiz, *La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad* (Madrid: Editorial Dykinson, 2005).

privacidad y la divulgación de la información con el objetivo de establecer límites entre ambas esferas y destacar la necesidad de proteger a los individuos de las injerencias de los medios de información[8].

La privacidad fue poco a poco limitándose como derecho y evolucionando con diferentes matices. En los años 60 del siglo XX, Alan F. Westin definió al *right to privacy*, como el derecho que tienen los individuos de controlar su propia información y de decidir a quién y cómo la comparten[9]. En 1977, Urabayen hizo notar que el *right to privacy*, entendido como el derecho a ser dejado en paz o a estar solo, pasó de la esfera de los derechos de propiedad a la esfera de los derechos de la personalidad[10].

Dentro del derecho a la privacidad, la doctrina empezó a preocuparse por el peligro que implicaba la facilidad de acceso a la información debido al desarrollo tecnológico y los riesgos que el mal uso de datos personales podría suponer. Al respecto, Antonio Pérez destacó que la privacidad es un derecho amplio y dinámico porque puede verse afectado con el mal manejo de la información de cada persona[11].

Por su parte, Vittorio Frosini explicó que el control electrónico de información como: documentos de identificación, datos fiscales, registros de crédito o reservas de viaje son muestras del riesgo de la informática en la seguridad individual y social de la vida cotidiana de las personas[12]. De esta forma, se empezó a delinear a la protección de datos como un derecho fundamental e independiente del derecho a la privacidad.

Al mismo tiempo en que se iba formando la protección de datos como un derecho autónomo, las legislaciones a nivel mundial reforzaban sus mecanismos de respeto a la privacidad e implementaban garantías para un tratamiento de datos adecuado. Víctor Cazurro, pone de ejemplo la adopción de *Privacy Act* de 1974, en Estados Unidos, que coincidió con la dimisión del presidente Richard Nixon debido al escándalo sobre espionaje de *Watergate* en el que estuvo vinculado[13].

---

[8] Jonathan López-Torres, "Antecedentes internacionales en materia de privacidad y protección de datos personales", *Journal of International Law* 5, núm. 2 (2014), 103–17.
[9] Alan F Westin, "Privacy and Freedom", *Washington and Lee Law Review* 25, núm. 166 (1968), https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20/.
[10] Miguel Urabayen Cascante, *Vida privada e información. Un conflicto permanente* (Pamplona: Eunsa, 1977).
[11] Antonio Enrique Pérez Luño, *La tercera generación de derechos humanos* (Pamplona: Editorial Aranzadi, S.A., 2006).
[12] Vittorio Frosini, *Cibernética, derecho y sociedad*, trad. Carlos A. Salguero-Talavera y Ramón L. Soriano Díaz (Madrid: Editorial Tecnos S.A., 1982).
[13] Víctor Cazurro Barahona, *Antecedentes y fundamentos del Derecho a la protección de datos*, 1era ed. (Barcelona: Bosch Editor, 2020).

A pesar de que la protección de datos era vista esencialmente como una estrategia para facilitar el flujo internacional de información y fomentar el desarrollo comercial transnacional, Artemi Rallo indica que, durante los años setenta "fue forjándose un emergente derecho de protección de datos en las legislaciones"[14]. Los Estados, especialmente en Europa, empezaron a incorporar en sus cartas fundamentales a la protección de datos como derecho autónomo e independiente a la privacidad.

Para Murillo de la Cueva y Piñar, muchas situaciones de invasión a la libertad es consecuencia del surgimiento de las nuevas tecnologías, de modo que debe otorgarse importancia a la protección de datos de carácter personal como un derecho[15]. Hoy en día, a nivel doctrinario y en la mayoría de las legislaciones se le da el nivel de fundamental al derecho de protección de datos y se le caracteriza como independiente del derecho a la intimidad o privacidad. De hecho, como menciona Luis Ordóñez, garantizar la protección de datos significa amparar el derecho a la intimidad en sí mismo[16].

3. Teorías sobre la protección a la privacidad e intimidad

El derecho a la protección de datos personales se ha forjado a través del desarrollo de teorías que tratan de enmarcar los ámbitos en los que la intimidad se ve afectada. Como indica Nisa Ávila, la teorización sirve para tener en cuenta distintas visiones y optar por la que mejor justifique la protección de datos personales[17]. Se presenta, a continuación, cuatro perspectivas teóricas para delimitar este trabajo de investigación.

Con una perspectiva civilista de los derechos de la personalidad, emerge la *Sphärentheorie* o teoría las esferas, atribuida al alemán Heinrich Hubmann[18]. Según esta teoría, los datos se encuentran distribuidos en tres esferas. En la primera, *privatsphäre*, se ubican aquellos datos de la vida privada que el titular no tiene problema en dar a conocer.

---

[14] Artemi Rallo Lombarte, "El nuevo derecho de protección de datos", *Revista Española de Derecho Constitucional*, núm. 116 (2019), 45–74, https://doi.org/10.18042/cepc/redc.116.02.

[15] Pablo Lucas Murillo de la Cueva y José Luis Piñar Mañas, *El derecho a la autodeterminación informativa* (Madrid: Fundación Coloquio Jurídico Europeo, 2009).

[16] Luis Ordóñez Pineda, "La protección de datos personales en los estados que conforman la Comunidad Andina: estudio comparado y precisiones para un modelo interamericano de integración", *UASB-E Foro: revista de derecho*, núm. 27 (2017), 83–114.

[17] Javier Antonio Nisa Ávila, *La Inteligencia artificial, IOT y data mining: una nueva perspectiva jurídica de la teoría del mosaico* (Lefebvre, 2021).

[18] Pablo Pascual Huerta, "La génesis del derecho fundamental a la protección de datos personales" (Tesis doctoral, Madrid, Universidad Complutense de Madrid, 2017), https://eprints.ucm.es/id/eprint/43050/1/T38862.pdf.

En la segunda, *vertravensphäre*, se encuentran datos confidenciales que el titular puede, o no, darlos a conocer según sea su voluntad. La tercera esfera, *gehimsphäre*, contiene los datos más íntimos y secretos del titular, quien no los podría dar a conocer ni con su propia autorización[19]. De modo que, existiría afectaciones a la intimidad si se involucran los datos de la esfera más interna, los demás datos serían irrelevantes[20].

En contraposición con la teoría de las esferas, se impone la teoría de mosaico formulada por Fulgencio Madrid Conesa[21]. Según esta teoría, hay una línea delgada que separa los datos privados de los públicos y para identificar la existencia de una afectación a la privacidad, se deben observan los datos de forma conjunta como si formaran un mosaico. Como explica Carlos Ruiz, algunos datos *a priori*, observados de forma aislada, pueden parecer irrelevantes, pero en conexión con otros, podría deducirse información importante, como la personalidad de un ciudadano[22].

También, se habla en doctrina de la teoría modular, la cual critica a la teoría de Madrid Conesa por ser una representación estática de los datos. Esta teoría, explicada por Javier Nisa, propone un escenario dinámico en el que los datos se procesan "como si fueran combustible para una máquina que se dedica a recrear la vida privada de los individuos con diferentes finalidades gubernamentales o comerciales"[23]. Concebir a los datos personales de esta forma, hace más exigente su tratamiento y más graves las sanciones por vulneraciones, entrando incluso, en el ámbito penal.

Finalmente, la cuarta teoría denominada *restricted access/limited control* fue acuñada por Hernan Tavani en el 2007 en el sistema anglosajón. Él hace una diferenciación entre pérdida de privacidad e invasión de la privacidad, explicando que solo en el segundo caso los datos serían objetos de protección por el derecho. Así mismo, distingue las situaciones privadas naturales de las situaciones privadas normativas, siendo las últimas las que merecen protección[24].

---

[19] Javier Antonio Nisa Ávila, *La Inteligencia artificial, IOT y data mining: una nueva perspectiva jurídica de la teoría del mosaico*.
[20] Eugenio Lanzadera Arencibia, "La eficacia del derecho a la intimidad en el entorno digital y su protección. Especial referencia a la relación laboral" (Tesis doctoral, Madrid, Universidad Autónoma de Madrid, 2017), http://hdl.handle.net/10486/680544.
[21] Fulgencio Madrid Conesa, *Derecho de la intimidad, informática y estado de derecho*, Colección de estudios Serie minor / Instituto de Criminologia y Departamento de Derecho Penál 7 (Valencia: Universidad de Valencia, 1984).
[22] Carlos Ruiz Miguel, "En torno a la protección de los datos personales automatizados", *Revista de estudios políticos*, núm. 84 (1994), 237–64.
[23] Javier Antonio Nisa Ávila, *La Inteligencia artificial, IOT y data mining: una nueva perspectiva jurídica de la teoría del mosaico, 30*.
[24] Hernan Tavani, "Philosophical theories of privacy: implications for an adequate online privacy policy", *Metaphilosophy* 38, núm. 1 (2007), 1–22.

Este trabajo de investigación se adhiere a la teoría modular como marco teórico, a partir del cual, se analiza la transferencia internacional de datos personales y sus estándares de aplicación, por ser la que más se adecúa a la realidad de la era digital, a la visión europea de protección de datos y a su concepción como derecho fundamental. Además, porque esta teoría permite entender la responsabilidad penal de las instituciones como resultado de una vulneración de dicho derecho.

4. Marco normativo

La regulación de protección y transferencia internacional de datos personales, TIDP, ha estado liderada por Europa y Estados Unidos. Sin embargo, es en Europa donde se ha adoptado un sistema más garantista, lo que ha hecho que tome la delantera a nivel internacional. Con base al modelo europeo, los Estados del resto del mundo han adaptado sus propias legislaciones. A continuación, se presenta la regulación normativa de la TIDP a nivel internacional, regional y local.

Primero, a nivel internacional sobresale el Reglamento General de Protección de Datos, RGPD, adoptado por la Unión Europea, UE, el 27 de abril de 2016, pero vigente desde 2018. Las características más relevantes de esta norma, a juicio de Andoni Polo Roca, son: (i) establece un sistema de protección de datos destallado y actualizado; (ii) tiene alcance general obligatorio para sus miembros consiguiendo la uniformidad legislativa a nivel comunitario; (iii) perfecciona el régimen de la TIDP a través de las decisiones de adecuación, normas corporativas vinculantes y códigos de conducta; y (iv) desarrolla el concepto de 'nivel adecuado' de protección como condición necesaria para transferir datos a un tercer país[25].

Al ser de gran alcance el RGPD europeo, el resto del mundo ha tenido que observar en sus legislaciones internas los conceptos y estándares que se exigen en él. En Estados Unidos, la protección de datos personales no se recoge en una legislación específica[26]. El instrumento jurídico más importante en la materia, hasta este momento, es el *California Consumer Privacy Act* ratificado el 28 de junio de 2018 y vigente desde

[25] Andoni Polo Roca, "Las transferencias internacionales de datos. Regulación actual y su incidencia en las relaciones exteriores de la Unión Europa", *Revista Aragonesa de Administración Pública*, núm. 57 (2021), 325–69.

[26] Albert Castellanos Rodríguez, "El régimen jurídico de las transferencias internacionales de datos personales. Especial mención al marco regulatorio Privacy Shield", *Institut de Ciències Polítiques i Socials (ICPS)*, núm. 30 (2017), 5–34.

2020[27]. Este instrumento está enfocado en proteger, sobre todo, a los consumidores de gigantes tecnológicos que tienen sede en California como Google y Facebook[28]. A pesar de que sigue la tendencia del RGPD, tiene ciertos vacíos en cuanto a la transferencia internacional de datos.

A nivel latinoamericano, no existe integración jurídica en esta materia. A pesar de que la Red Iberoamericana de Protección de Datos ha hecho esfuerzos para lograr en la región un escenario con iniciativas y proyectos comunes, a través de la adopción de estándares de protección de datos personales, no dejan de ser "meras buenas prácticas que quedan, en lo que se refiere a su cumplimiento, sujetas a la decisión de los Estados, los cuales pueden o no seguir dichos criterios"[29].

Por un lado, están países como Argentina, Uruguay, México, Perú y Colombia, que desarrollaron sus normas de protección de datos ya en los años 2000; con la adopción del RGPD han estado en proceso de reforma de leyes para seguir sus lineamientos. Por otro lado, están los países que no cuentan con normativa ni iniciativas legislativas en materia de protección de datos como Venezuela[30].

Finalmente, Ecuador hace solo un año, luego de dos iniciativas fallidas, dejó de formar parte del grupo de países sin reglamentación específica con la entrada en vigencia de la LOPDP. La primera iniciativa en 2010 fue archivada porque se planteó como ley ordinaria cuando en el fondo contenía derechos fundamentales necesarios de ser desarrollados en una ley orgánica[31]. La segunda iniciativa en 2016 tuvo numerosas críticas por imprecisiones conceptuales, entre otras cosas, porque no se alineaba a las exigencias europeas en materia de transferencia de datos personales[32].

A mediados de enero de 2019, la actual Dirección Nacional de Registros Públicos, DINARP[33], dio a conocer el anteproyecto de la ley a través de su página web.

---

[27] Christian Razza, *La transferencia internacional de datos personales en Ecuador. Protección frente al libre flujo*, ed. Susana Salvador Crespo, 1era ed. (Quito: Universidad de las Américas, 2021).
[28] Ibidem.
[29] José Francisco Santamaría Ramos, "El principio de responsabilidad proactiva: una oportunidad para un mejor cumplimiento de la normativa en materia de protección de datos de carácter personal en el ámbito latinoamericano", *Derecho PUCP*, núm. 85 (2020), 139–74, https://doi.org/10.18800/derechopucp.202002.005.
[30] Ibidem.
[31] Bernadette Califano, "Análisis del proceso de debate de iniciativas legales sobre protección de datos personales y sus conflictos con el derecho a la libertad de expresión. Los casos de Argentina y Ecuador", *Centro de Estudios en Libertad de Expresión y Acceso a la Información de Universidad de Palermo*, (2021).
[32] Luis Enríquez Álvarez, "Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales", *UASB-E Foro: revista de derecho*, núm. 27 (2017), 43–61.
[33] DINARP es el nombre actual de la anterior Dirección Nacional de Registro de Datos Públicos, DINARDAP.

La Asamblea aprobó el proyecto en segundo debate del 10 de mayo de 2021 y, finalmente, se publicó en el Registro Oficial el 26 de ese mismo mes. Hoy en día, está en proceso de revisión el proyecto de reglamento a la ley y se está a la espera de la designación del Superintendente de Protección de Datos y la configuración de la institución que encabezará.

La LOPDP recoge, en el capítulo IX, los conceptos y estándares en materia de transferencia internacional de datos personales del RGPD, pero con ciertas distinciones. Por eso, en la siguiente sección se revisa la conceptualización de la transferencia internacional de datos, para después, hacer un análisis comparativo de los estándares de protección establecidos en el RGPD con los que incluyó el legislador ecuatoriano en la LOPDP.

5. Delimitación de la transferencia internacional de datos personales

Cuando los Estados empezaron a regular el derecho de protección de datos, durante la década de los setenta, se dieron cuenta de la necesidad de desarrollar reglas comunes para que los esfuerzos internos de protección no se desvanezcan en los intercambios comerciales internacionales [34] . En 1980, la Organización para la Cooperación y el Desarrollo Económico, OCDE, se refirió al concepto de flujo transfronterizo de datos personales como el desplazamiento de datos fuera de las fronteras nacionales, que debe ser regulado para fomentar el desarrollo económico transnacional[35].

Luego, el Consejo de Europa definió al flujo transfronterizo de datos como la "transmisión a través de las fronteras nacionales, por cualquier medio, datos de carácter personal que sean objeto de un tratamiento automatizado o reunidos con el fin de someterlos a ese tratamiento"[36]. En 1990, la Asamblea General de Naciones Unidas lo entendió como un principio, según el cual, la información debe poder circular libremente en el interior de aquellos países que ofrecen garantías comparables de protección a la vida privada[37].

[34] Nelson Remolina-Angarita, "¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?", *International Law: Revista Colombiana de Derecho Internacional* 8, núm. 16 (2010), 489–524.
[35] Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales de la Organización para la Cooperación y el Desarrollo Económico, 23 de septiembre de 1980.
[36] Convenio n.º 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, Estrasburgo, 28 de enero de 1981.
[37] Directrices para la regulación de los ficheros informatizados de datos personales. Resolución A/RES/45/95 de la Asamblea General de las Naciones Unidas, 14 de diciembre de 1990.

En octubre de 1995, el Parlamento Europeo y el Consejo de Europa elaboraron la Directiva 95/46/CE, sobre el tratamiento de datos personales y su libre circulación. En dicha Directiva se diferenciaron dos niveles de protección en la transferencia internacional de datos: el nivel equivalente, cuando el intercambio sucede entre países miembros de la UE; y el nivel adecuado, cuando se involucra un país ajeno a la Unión[38]. El nivel adecuado de protección debía ser declarado previamente por la Comisión Europea, CE, para que efectivamente el país ajeno sea receptor de datos. Esta Directiva fue derogada con la entrada en vigencia del RGPD.

El RGPD perfeccionó las reglas de transferencia internacional. En él, se distinguen dos conceptos: transferencia de datos transfronteriza y transferencia internacional de datos. El primero concepto, de hecho, es lo que la Directiva 95/46/ce llamaba nivel equivalente. Es decir, la transmisión desde y hacia organizaciones ubicadas en más de un Estado miembro de la UE[39]. El segundo, se refiere a la transmisión que se efectúa desde un lugar de la UE hacia un país u organización externa a ella. La transferencia internacional y sus estándares se encuentran en el capítulo V del RGPD. A continuación, se presentan cada uno de ellos.

6. Estándares de protección en la TIDP

El artículo 44 del RGPD, señala que solo es posible la transferencia de datos si el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el Reglamento, "incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional"[40]. Es importante destacar desde este momento que las transferencias ulteriores no se encuentran incluidas en la LOPDP, lo cual supone una desventaja al Ecuador como país receptor de datos personales según Christian Razza[41].

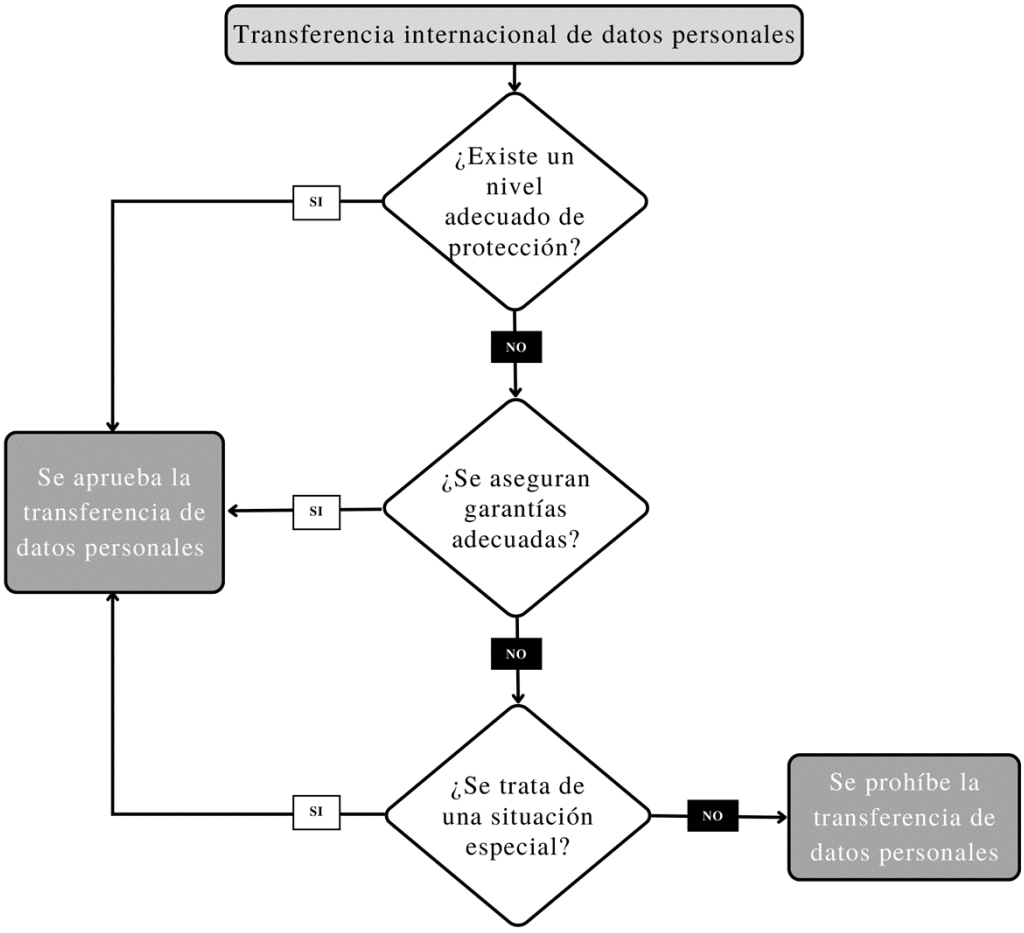
En los siguientes artículos se detallan las condiciones para la TIDP. A modo de esquematizarlas, Razza las clasifica en tres niveles de protección: 1) nivel adecuado; 2)

[38] Directiva 95/46/CE del Parlamento Europeo y del Consejo 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. Diario Oficial de las Comunidades Europeas 281/31, 24 de octubre de 1995.
[39] Reglamento General de Protección de Datos UE 2016/679, Diario Oficial de la Unión Europea 119/63, 27 de abril de 2016.
[40] Artículo 44, Reglamento UE 2016/679.
[41] Christian Razza, *La transferencia internacional de datos personales en Ecuador. Protección frente al libre flujo*.

garantías adecuadas; y 3) normas corporativas vinculantes[42]. De forma similar, Andoni Polo Roca, clasifica a estas condiciones en tres secciones, y añade como una cuarta sección a las "excepciones por situaciones específicas" que se encuentran en el artículo 49 del Reglamento[43].

En realidad, las normas corporativas vinculantes se incluyen en el nivel de garantías adecuadas, por lo tanto, no debería contar como un nivel independiente de la forma en que lo hace Razza. En cambio, las situaciones específicas del artículo 49 si suponen un tercer nivel de protección de TIDP, como efectivamente indica Roca. Entonces, armonizando a ambos autores y siguiendo el RGPD, se presenta el siguiente diagrama de flujos resumiendo los tres estándares de transferencia internacional.

Gráfico No. 1 Estándares en la transferencia internacional de datos personales



Fuente: elaboración propia.

[42] Christian Razza, *La transferencia internacional de datos personales en Ecuador. Protección frente al libre flujo*.
[43] Andoni Polo Roca, "Las transferencias internacionales de datos. Regulación actual y su incidencia en las relaciones exteriores de la Unión Europa".

Como se puede deducir del gráfico, el primer estándar es el nivel más alto e ideal para la TIDP y las situaciones especiales son excepcionales, casos muy puntuales en los que no existe decisión de adecuación ni garantías adecuadas. Estas condiciones de protección fueron incluidas en la LOPDP con sus respectivos matices. Por eso, en el siguiente apartado se hace una comparación entre ambos cuerpos normativos.

6.1. Primer estándar: decisión de nivel adecuado de protección

Como regla general, la TIPD será autorizada mediante decisión de adecuación dictada por la CE que certifique que el país u organización receptora tiene un 'nivel de protección adecuado'. A pesar de que, ni la Directiva 95/46/CE ni el RGPD definen el concepto de 'nivel adecuado', el Tribunal de Justicia de la Unión Europea, TJUE, en sentencia sobre el caso *Maximilian Schrems* del 6 de octubre de 2015 se pronunció indicando que el término 'adecuado' no implica exigir que el tercer país garantice un nivel de protección 'idéntico' al de la UE, sino que en su legislación interna y en sus compromisos internacionales se garantice "un nivel de protección de las libertades y derechos fundamentales 'sustancialmente equivalente' al garantizado en la Unión […]"[44]

La idea de que una legislación tenga un nivel de protección sustancialmente equivalente no es lo mismo a decir que tiene un nivel 'exacto' al que proporciona la legislación europea, sino más bien semejante[45]. En dicha sentencia, además, el TJUE instó a entender las decisiones de adecuación presunciones de garantía de protección de datos personales, mas no como una decisión definitiva, porque podrían impugnarse y revocarse si ya no se constata el nivel adecuado de protección de datos en el respectivo país[46]. Justamente, en esa ocasión, indica Itziar Sobrino, se anuló el *Safe Harbor Agreement*[47] celebrado entre la UE y los Estados Unidos por falta de obligatoriedad del instrumento y

[44] Maximillian Schrems c. Data Protection Commissioner, Tribunal de Justicia de la Unión Europea, 6 de octubre de 2015, párr. 73.
[45] Miguel Recio Gayo, "Nivel adecuado para transferencias internacionales de datos", *Derecho PUCP*, núm. 83 (2019), 207–40, https://doi.org/10.18800/derechopucp.201902.007.
[46] Maximillian Schrems c. Data Protection Commissioner, párr.83.
[47] El *Safe Habor* o "Puerto Seguro" fue el acuerdo entre Estados Unidos y la UE para el intercambio de datos personales libremente entre ellos. Con su invalidez, miles de empresas buscaron métodos alternativos para no interrumpir sus relaciones comerciales, pero hubo incertidumbre jurídica en las operaciones mercantiles hasta que se aplicara el *Privacy Shield* de 2016. Al respecto, en 2020 también se anuló dicho acuerdo y en octubre de 2022 el presidente Joe Biden firmó la orden para un nuevo tratado. *Ver* Leticia López Lapuente, "Las transferencias de datos a EE.UU.: la transición del Safe Harbor al Privacy Shield y un paso más allá.", *Actualidad Jurídica Uría Menéndez*, 2017, 36–38; The White House, "Fact Sheet: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework", The White House, el 7 de octubre de 2022, https://n9.cl/3rmby (último acceso:10/10/2022).

por considerar que no demuestra que Estados Unidos garantice un nivel adecuado de protección[48].

En el artículo 45.2 del RGPD se establecen los elementos que debe tener en cuenta la CE para evaluar el nivel de adecuación del tercer país. Adicionalmente, el Comité Europeo de Protección de Datos, publicó varias directrices para la CE y para terceros países que se proponen obtener una decisión de adecuación. Entre ellas, se encuentran las restricciones a transferencias ulteriores[49]. Esto es cuando el tercer país u organización que en un inició receptó datos personales, se convierte en emisor de esa información a un siguiente país u organización. En este sentido, se exige que esta transferencia posterior no distorsione el nivel de protección previsto en la UE, que tenga fines específicos, limitados y fundamento jurídico.

Ahora bien, en el caso de Ecuador, el artículo 56 de la LOPDP permite la transferencia internacional de datos personales a países, organizaciones y personas jurídicas fuera del país siempre y cuando "brinden niveles adecuados de protección y que se ajusten a la obligación de cumplimiento y garantía de estándares reconocidos internacionalmente conforme a los criterios establecidos en el Reglamento a la ley"[50]. A grandes rasgos, la norma reproduce el concepto de nivel adecuado de protección del RGPD. También, añade el término de personas jurídicas, que en el caso del RGPD, están incluidas como organizaciones.

Así mismo, la LOPDP establece que la Autoridad de Protección de Datos Personales es la encargada de declarar, mediante resolución motivada, la existencia o no de un nivel adecuado de protección en el país con el que se pretende intercambiar datos. Esta autoridad le corresponde al aún no posicionado Superintendente de Protección de Datos.

Es importante hacer énfasis que la transferencia ulterior de datos personales no se encuentra desarrollada en la ley. El problema de esto radica en las dificultades que va a tener el Ecuador para ser catalogado como un país con nivel adecuado de protección, pues uno de los requisitos que debe observar la CE para dictar decisión de adecuación

[48] Itziar Sobrino García, "Las decisiones de adecuación en las transferencias internacionales de datos. El caso del flujo de datos entre la Unión Europea y Estados Unidos", *Revista de Derecho Comunitario Europeo*, núm. 68 (el 28 de abril de 2021): 227–56, https://doi.org/10.18042/cepc/rdce.68.07.

[49] Directrices 2/2020 relativas a la aplicación del artículo 46, apartado 2, letra a), y del artículo 46, apartado 3, letra b), del Reglamento 2016/679 con respecto a las transferencias de datos personales entre autoridades y organismos públicos del EEE y de fuera de este del Comité Europeo de Protección de Datos, 15 de diciembre de 2020.

[50] Artículo 56, Ley Orgánica de Protección de Datos Personales [LOPDP]. R.O. Suplemento 459 de 26 de mayo de 2021.

favorable es, justamente, que el país receptor cuente con reglas para las transferencias ulteriores de datos. De todas formas, se espera que la definición de nivel adecuado de protección, el desarrollo de los criterios para determinarla y las restricciones para las transferencias ulteriores, se incluyan en el reglamento a la ley.

Tabla comparativa No. 1 Transferencia de datos según nivel de adecuación

	RGPD	LOPDP
Autoridad encargada de emitir decisión	Comisión Europea	Superintendencia de Protección de Datos
Transferencia ulterior de datos	Se incluye	No se incluye
Definición de nivel adecuado	Sin definición, pero desarrollada por el TJUE	Sin definición
Sujetos que intervienen	Países y organizaciones	Países, personas jurídicas en general y organizaciones

Fuente: Elaboración propia, a partir del artículo 45 del RGPD y 56 de la LOPDP.

6.2. Segundo estándar: garantías adecuadas

Las garantías adecuadas en el RGPD se mencionan en los considerandos preliminares 107 y 108. Se explica que, si la CE determina que un tercer país no cuenta con un nivel adecuado de protección, debe prohibirse la TIDP a menos que se otorguen las garantías adecuadas para el interesado. Algunos ejemplos de estas garantías son: normas corporativas vinculantes, cláusulas tipo de protección de datos, instrumentos vinculantes entre autoridades públicas, códigos de conducta, mecanismos de certificación, acuerdos administrativos[51].

Además, se exige que las garantías adecuadas en los terceros países observen los requisitos establecidos en el RGPD y que, en caso de afectación al titular de datos, otorguen la posibilidad de reclamar indemnización en la UE o en el tercer país. El artículo 46 del RGPD enfatiza la necesidad de que las garantías adecuadas sean acompañadas de la existencia de derechos concretos exigibles y acciones legales efectivas para los interesados.

[51] Considerando número 108, Reglamento UE 2016/679.

Estas garantías se clasifican en dos grupos: por un lado, aquellas que no requieren autorización expresa de una autoridad de control; y, por otro lado, las garantías que si necesitan dicha autorización. Por autoridad de control se refiere a la institución a cargo de la protección de datos personales en cada país, en el caso de España, por ejemplo, es la Agencia Española de Protección de Datos, AEPD.

Al respecto, debe hacerse una aclaración. No es lo mismo autorización que aprobación de la autoridad de control. Cuando se habla de autorización significa que cada vez que se realice una transferencia internacional de datos, las empresas tendrían que empezar un nuevo trámite administrativo pidiendo autorización a la autoridad; esto sería un obstáculo para el tráfico jurídico[52]. En cambio, la aprobación se refiere a la verificación previa por la autoridad de control para que, una vez aprobadas las garantías, en adelante se pueda intercambiar libremente datos sin trámites adicionales.

Las garantías adecuadas que no requieren autorización expresa de una autoridad de control son: 1) instrumentos jurídicamente vinculantes y exigibles entre las autoridades u organismos públicos; 2) normas corporativas vinculantes; 3) cláusulas tipo; 4) códigos de conducta; y 5) mecanismos de certificación. Estos últimos son expedidos por organismos de certificación con especialización en materia de protección de datos.

Por instrumentos jurídicamente vinculantes se refiere al ámbito en que las administraciones públicas celebran acuerdos vinculantes y exigibles en los que haya transferencia internacional de datos, por lo tanto, como explica Roca, se limita al ámbito público[53]. En el caso de que estos acuerdos no sean vinculantes, necesitarán de autorización de la autoridad competente.

Las normas corporativas vinculantes y los códigos de conducta son revisadas a profundidad en el apartado 7.1 y 7.2 de este trabajo. Las cláusulas tipo no son más que cláusulas de protección que se incluyen en un contrato celebrado entre el exportador y el importador de datos. Estas cláusulas adoptadas voluntariamente por las entidades de derecho privado son redactadas y aprobadas, o bien, solo por la CE o por la autoridad de control y la CE[54].

Es decir, la CE difunde un conjunto de cláusulas tipo que están aprobadas para ser utilizadas sin necesidad de autorización posterior por la autoridad de control

[52] Andoni Polo Roca, "Las transferencias internacionales de datos. Regulación actual y su incidencia en las relaciones exteriores de la Unión Europa".
[53] Ibidem.
[54] Ibidem.

competente. El 4 de junio de 2021 se expidió la Decisión de Ejecución UE 2021/914 más actual con la lista de cláusulas tipo[55]. También, las autoridades de control de cada país pueden preparar cláusulas tipo que deben ser aprobadas por la CE para que sean jurídicamente válidas a efectos del RGPD[56].

Las garantías adecuadas que requieren autorización de la autoridad de control competente son: 1) cláusulas que se incluyan en contratos celebrados entre responsables y encargados de protección de datos en ambos países; y 2) las disposiciones que se incorporen en acuerdos administrativos no vinculantes, por ejemplo, memorandos de entendimiento, entre las autoridades u organismos públicos[57]. Con respecto a la primera, la Decisión de Ejecución UE 2021/914 contiene directrices que deberán tomar en cuenta las entidades de derecho privado para incluir cláusulas de protección de datos en sus contratos.

En el caso de la LOPDP, las garantías adecuadas se mencionan en el artículo 57. A diferencia del RGPD, no se enlistan los tipos de garantías. En cambio, prescribe los criterios que deben observarse para que sea posible la transferencia de datos al país, organización o territorio económico que no haya sido considerado con nivel adecuado de protección por la Superintendencia.

Son tres criterios que la LOPDP exige para la transferencia internacional de datos mediante garantías adecuadas: 1) que se garantice el cumplimiento de principios, derechos y obligaciones con un estándar igual o mayor a la normativa ecuatoriana; 2) que existan de acciones administrativas o judiciales permanentes para tutelar el derecho a la protección de datos; y 3) que sea posible solicitar reparación integral[58]. Además, la norma señala que la transferencia de datos debe sustentarse en un instrumento jurídico vinculante que contemple los estándares antes mencionados y los que considere oportunos la Superintendencia.

[55] Decisión de Ejecución (UE) 2021/914 de la Comisión relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, 4 de junio de 2021.
[56] Vicente Guasch Portas, "La transferencia internacional de datos de carácter personal", *Revista de Derecho de la UNED*, núm. 11 (2012), 413–53, https://doi.org/10.5944/rduned.11.2012.11139.
[57] Artículo 46, Reglamento UE 2016/679.
[58] Artículo 57, LOPDP.

Tabla comparativa No.2 Garantías adecuadas de protección de datos personales

<table>
<tr><th colspan="2">RGPD</th><th>LOPDP</th></tr>
<tr><td colspan="2">Las garantías adecuadas se clasifican según requieran o no autorización:</td><td rowspan="3">No enlista los tipos de garantías, pero establece criterios para la transferencia internacional de datos:
1) Que exista garantía de cumplimiento de estándares iguales o mayores al ecuatoriano.
2) Acciones administrativas y judiciales para tutelar la protección de datos.
3) Posibilidad de solicitar reparación integral.</td></tr>
<tr><td>Con autorización</td><td>Sin autorización</td></tr>
<tr><td>1) Cláusulas contractuales.
2) Acuerdos administrativos.</td><td>1) Instrumentos vinculantes entre autoridades públicas.
2) Normas corporativas vinculantes.
3) Cláusulas tipo.
4) Códigos de conducta.
5) Mecanismos de certificación.</td></tr>
</table>

Fuente: elaboración propia, a partir del artículo 46 del RGPD y 57 de la LOPDP.

6.3. Tercer estándar: situaciones especiales

En el artículo 49 del RGPD se enlistan siete situaciones en las que es posible la transferencia de datos a falta de decisión de adecuación y de garantías adecuadas de protección. La LOPDP, por su parte, los denomina casos excepcionales de transferencias o comunicaciones internacionales y enumera once de ellos.

Tabla comparativa No. 3 Situaciones excepcionales para el intercambio de datos

	Situación	RGPD	LOPDP
1	Cuando existe consentimiento explícito del titular de datos previo aviso de los posibles riesgos de transferencia.	✓	✓
2	Para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para ejecución de medidas precontractuales a solicitud del interesado.	✓	✓

3	Para la celebración de o ejecución de un contrato entre el responsable de tratamiento y otra persona física o jurídica.	✓	×
4	Por razones importantes de interés público.	✓	✓
5	Para la formulación, ejercicio o defensa de reclamaciones[59].	✓	✓
6	Para proteger los intereses vitales del interesado o de otras personas cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento.	✓	✓
7	Desde un registro público para facilitar la información a las personas que acrediten interés legítimo solo en la medida que se cumplan las condiciones de la UE.	✓	×
8	En operaciones bancarias y bursátiles.	×	✓
9	Para el cumplimiento de compromisos en procesos de cooperación internacional entre Estados.	×	✓
10	Como cooperación dentro de la investigación de infracciones.	×	✓
11	Para la colaboración judicial internacional	×	✓
12	Para el cumplimiento de una obligación legal o regulatoria.	×	✓
13	Para el cumplimiento de competencias institucionales.	×	✓

Fuente: elaboración propia, a partir del artículo 49 del RGPD y 60 de la LOPDP.

La LOPDP introduce seis situaciones que no contempla el RGPD dentro del artículo sobre situaciones especiales, pero muchas de ellas se encuentran en artículos posteriores. Por ejemplo, tanto la cooperación judicial internacional como el cumplimiento de compromisos en procesos de cooperación internacional se encuentra en el artículo 50 del RGPD.

Una vez revisado el régimen de transferencia internacional de datos personales en la normativa europea y ecuatoriana, a continuación, se analiza la responsabilidad proactiva como principio transversal del sistema de protección de datos personales; así como las normas corporativas vinculantes y códigos de conducta como mecanismos eficientes para la autorregulación corporativa.

[59] En la LOPDP se añade la formulación de acciones administrativas o jurisdiccionales, así como los recursos.

7. Principio de responsabilidad proactiva y autorregulación

En la LOPDP, el principio de responsabilidad proactiva se ubica, primero, en el artículo 10.k) dentro del capítulo II sobre principios generales del sistema ecuatoriano de protección de datos, el cual establece el deber del responsable del tratamiento de:

> acreditar la implementación de mecanismos para la protección de datos personales pudiendo valerse de estándares, mejores prácticas, esquemas de auto y coregulación, códigos de protección, sistemas de certificación, sellos de protección de datos personales o cualquier otro mecanismo que se determine adecuado a los fines, la naturaleza del dato personal o el riesgo del tratamiento[60].

En efecto, el alcance de este principio es el de no limitarse al cumplimiento de la normativa vigente, sino que los responsables y encargados estén en condición de demostrar que han actuado de forma diligente en el tratamiento de datos. En pocas palabras, "no incumplir ya no es suficiente"[61] porque se busca un real compromiso para garantizar, por un lado, el respeto a los derechos de los interesados y, por otro lado, facilitar el flujo de datos entre corporaciones, entes públicos y particulares[62].

Luego, el capítulo VIII está dedicado enteramente a este principio. Se establece la autorregulación de las instituciones mediante la adopción voluntaria de: códigos de conducta, certificaciones, sellos y marcas de protección y/o cláusulas tipo[63]. Llama la atención que estos mecanismos de transferencia de datos no se hayan mencionado en el artículo de garantías adecuadas, pero se los incluya en este capítulo. Precisamente, adoptar mecanismos de autorregulación es una forma de demostrar responsabilidad proactiva.

Las normas corporativas vinculantes y los códigos de conducta son las garantías adecuadas ejemplares en la autorregulación corporativa, a la vez, necesaria para observar el principio de responsabilidad proactiva[64]. Pero ¿por qué es importante que las empresas se comprometan con la autorregulación a través de estas garantías adecuadas? Porque el Ecuador no ha sido catalogado por la CE como un país seguro para la transferencia internacional de datos personales.

---

[60] Artículo 10.k), LOPDP.
[61] Fernando Biurrun Abad, 'Accountability' o responsabilidad activa en el Reglamento General de Protección de Datos", *Actualidad Jurídica Aranzadi*, 2017.
[62] Manuel Estepa Montero, "El principio de responsabilidad proactiva o rendición de cuentas como informador del régimen jurídico de la protección de datos de las personas físicas", *Anuario jurídico y económico escurialense*, núm. 55 (2022), 67–90.
[63] Artículo 52, LOPDP.
[64] Lokke Moerel, *Binding Corporate Rules. Corporate self-regulation of global data transfer*, 1era ed. (Oxford: Oxford University Press, 2012).

Las garantías adecuadas tienen una aplicación subsidiaria en la transferencia internacional de datos. Como se explicó, la regla general es que el país receptor cuente con una decisión de adecuación por la CE y, es en este punto en dónde el sistema ecuatoriano presenta complicaciones. A pesar, de que ya existe una ley específica en la materia, Ecuador está lejos de ser declarado país con un nivel adecuado de protección de datos por dos principales razones.

Primero, en la LOPDP no se observan directrices para la transferencia ulterior de datos. Sin perjuicio de que en el futuro reglamento a la ley se incluya, esto pone en desventaja al país para tener resolución positiva del CE, pues el artículo 44 del RGPD demanda a la legislación del país receptor contener reglas claras para las transferencias ulteriores. Añadiendo a esto, el trámite que se inicia ante la CE para ser catalogado como país con nivel adecuado de protección, con base en experiencia previa de otros países, según lo explica Remolina-Angarita, toma tiempo. De modo que, según el autor, es poca la probabilidad de obtener una resolución de adecuación en el corto o, hasta mediano plazo[65].

Incluso en el ámbito latinoamericano, legislaciones sobre protección de datos personales con más trayectoria que la ecuatoriana, no han sido del todo eficientes por falta de protección de datos auténtica en sus instituciones y debilidades en la actitud proactiva de los responsables del tratamiento[66]. De hecho, la CE solamente ha declarado a Argentina y Uruguay como países latinoamericanos que tienen nivel adecuado de protección de datos mediante las Decisiones 2003/490/CE y 2012/484/UE, respectivamente[67].

En segundo lugar, el sistema normativo e institucional sobre protección de datos en el país aún no se han constituido completamente. Esto empeora el escenario para ser considerados un país seguro para la transferencia internacional de datos. Por lo tanto, hasta que se fortalezca y perfeccione el sistema para contar con decisión de adecuación por la CE, el sector empresarial debe priorizar la adopción de garantías adecuadas mediante mecanismos de autorregulación, como los que a continuación se presentan.

[65] Nelson Remolina-Angarita, "¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?"
[66] José Francisco Santamaría Ramos, "El principio de responsabilidad proactiva".
[67] Juan José Gonzalo Domenech, "Las decisiones de adecuación en el Derecho europeo relativas a las transferencias internacionales de datos y los mecanismos de control aplicados por los estados miembros", *Cuadernos de Derecho Transnacional* 11, núm. 1 (2019), 350–71, https://doi.org/10.20318/cdt.2019.4624.

7.1. **Normas corporativas vinculantes**

Conocidas en inglés como *binding corporate rules, BCR*, son normas internas aplicables entre un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta con el objetivo de facilitar la transferencia internacional de datos personales y asegurar que los responsables y encargados de tratamiento de datos actúen de forma diligente, cuando el tercer país no cuenta con un nivel adecuado de protección.

Estas normas tienen una naturaleza mixta pues, por un lado, son redactadas por el grupo o unión de empresas; y, por otro, son aprobadas por la autoridad de control. Lokke Moerel indica, muy acertadamente, que las normas corporativas vinculantes sirven como puentes entre los sistemas jurídicos que no están al mismo nivel en materia de protección de datos personales[68]. Además, explica que han servido como "guías para programas modelo de cumplimento de protección de datos personales, incluso en las empresas que no transfieren datos a nivel internacional[69]"

Algunos de los elementos que deben especificar estas normas para considerarse válidas a efectos del RGPD son: (i) la estructura de datos del grupo o unión empresarial; (ii) los procedimientos de reclamación; (iii) mecanismos de verificación como, por ejemplo, auditorías; (iv) carácter jurídicamente vinculante interna y externamente, entre otros elementos[70]. De todas formas, es interesante analizar los escenarios de aplicación de este mecanismo de autorregulación.

El primer escenario en el que se establecen estas normas es entre entidades que tienen sede en diferentes partes del mundo, pero se encuentran dentro del mismo grupo empresarial. Como ejemplo, está el caso del Grupo Fujikura Automotive Europe, S.A.U, que fue la primera aprobación de normas corporativas vinculantes bajo el RGPD[71]. En este caso, la autoridad española de protección de datos concluyó que las normas adoptadas por el grupo empresarial cumplieron los requisitos del artículo 47 del RGPD, permitiendo la transferencia de datos desde España, Alemania, República Checha y Rumania, hacia Ucrania, Marruecos y Moldavia[72].

Un segundo escenario, que amplía el alcance de las normas corporativas vinculantes, es la posibilidad de invocarlas, no solo en un mismo grupo empresarial, sino

[68] Lokke Moerel, *Binding Corporate Rules. Corporate self-regulation of global data transfer*.
[69] Ibidem, 227 (traducción no oficial).
[70] Artículo 47, Reglamento UE 2016/679.
[71] Resolución de aprobación de las normas corporativas vinculantes del grupo Grupo Fujikura Automotive Europe (Grupo FAE). Expediente TI/00001/2020, 13 de marzo de 2020.
[72] Ibidem.

también en la unión de empresas que están asociadas por tener actividades económicas conjuntas. Al respecto, Lee Bygrave, indica que, a pesar de que no es clara la explicación de este escenario en el RGPD, se puede ejemplificar a través de la figura del *joint venture* o formación de alianzas entre empresas en la medida en la que sean estables como, por ejemplo, el sector de las aerolíneas[73].

Pues bien, el escenario de adoptar estas normas dentro del supuesto de unión de empresas dedicadas a una actividad económica conjunta lleva a plantearse la posibilidad de que las entidades nacionales puedan hacer una elección de jurisdicción o *forum* para que sea suficiente una sola aprobación de la autoridad de protección del país que cuente con un nivel adecuado de protección.

Es decir, si una empresa ubicada en Ecuador, y otra ubicada en España celebran una alianza por tener una actividad económica conjunta y quieren autorregularse en materia de protección de datos a través de normas corporativas vinculantes, la empresa ecuatoriana podría elegir subordinarse a la regulación europea y la aprobación de la AEPD debería ser suficiente para que las normas corporativas se entiendan aprobadas también en por la autoridad ecuatoriana.

En estos casos, la autoridad ecuatoriana de protección de datos, la Superintendencia, debería entender por aprobadas las normas corporativas vinculantes con base en la disposición del numeral 3 del artículo 57, según el cual, las garantías adecuadas deben observar los principios en el tratamiento de datos personales en estándares iguales o mayores a la normativa nacional vigente. España tiene un nivel de protección de datos personales mayor al del Ecuador, por lo tanto, se entendería que las normas corporativas vinculantes son válidas también dentro del país. Esta sería una solución para ante las falencias de la LOPDP.

La LOPDP se refiere a las normas corporativas vinculantes en el artículo 58. Nuevamente, se hace notar la falta de desarrollo conceptual en la norma. De todas formas, en este artículo se establecen las condiciones que deben reunir las normas corporativas para ser aprobadas por la Superintendencia. Entre ellas, que sean jurídicamente vinculantes, que contengan los datos específicos de cada entidad que forme parte del grupo empresarial; así como la existencia de mecanismos de reclamación, de verificación del cumplimiento mediante auditorías, de cooperación con la autoridad, entre otras. Todas éstas, recogidas del artículo 47 del RGPD.

[73] Lee A. Bygrave, *The EU General Data Protection Regulation (GDPR): a commentary*, ed. Christopher Docksey y Christopher Kuner (Oxford: Oxford University Press, 2020).

7.2. Códigos de conducta

Los códigos de conducta, explica la persona, tienen una relación de género a especie con las normas corporativas vinculantes. Es decir, un código de conducta puede llegar a ser una norma corporativa vinculante *per se,* si su contenido y proceso de aprobación cumple con el artículo 47 del RGPD[74]. De todos modos, son mecanismos voluntarios de autorregulación que consisten en una serie de reglas específicas encaminadas al correcto cumplimiento de la normativa. Además, son instrumentos de cumplimiento del principio de responsabilidad proactiva y demostrada según el RGPD[75].

Los códigos de conducta refuerzan la acreditación de diligencia en la actuación de los responsables y encargados del tratamiento. De hecho, es la manera en que las entidades pueden concretar el principio de responsabilidad proactiva y demostrar una actitud permanente en el cumplimiento de estándares de protección de datos. Con esta actitud de compromiso, las entidades incluso pueden servirse de los códigos de conducta como atenuantes a la responsabilidad civil y penal en casos de incumplimiento de la norma[76].

Al respecto de la responsabilidad penal de las personas jurídicas, es interesante el análisis de la implementación de un código de conducta, incluso, como eximente de responsabilidad. Manuel Estepa Montero explica, en el caso de España, que el Tribual Supremo le ha dado mucha importancia a la cultura del respeto al Derecho en la tarea de determinar la actuación relevante sujeta a sanción penal para una persona jurídica[77]. A juicio del Tribunal, "la presencia de mecanismos de control adecuados supondría la inexistencia misma de la infracción"[78], con lo que se conseguiría la exoneración de esa responsabilidad para evitar daños en la reputación de la entidad[79].

Sin embargo de esta discusión doctrinaria sobre los códigos de conducta como eximentes de responsabilidad penal, el legislador ecuatoriano definitivamente, en el artículo 52 de la LOPDP, excluye la posibilidad de que los mecanismos de

[74] Luis Alberto Montezuma Chávez, "Normas corporativas vinculantes y transferencias internacionales de datos personales: elementos para su reglamentación", *Revista de Derecho, comunicaciones y nuevas tecnologías. Universidad de los Andes*, núm. 8 (2012) 1–40.
[75] Agencia Española de Protección de datos, "Códigos de conducta", el 14 de junio de 2022, https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/codigos-de-conducta
[76] Manuel Estepa Montero, "El principio de responsabilidad proactiva o rendición de cuentas como informador del régimen jurídico de la protección de datos de las personas físicas".
[77] Ibidem.
[78] Ibidem, 74.
[79] Ibidem.

autorregulación constituyan eximentes de responsabilidad de dar cumplimiento a la ley. En el artículo 53 se establece el deber de la autoridad de control de promover la elaboración de códigos en los distintos sectores empresariales, tomando en cuenta las necesidades específicas de cada uno. En complemento, el artículo 54 habla de la utilidad probatoria de los mecanismos de autorregulación.

7.3. Cultura ética y responsabilidad social corporativa

Adela Cortina distingue la cultura ética corporativa de la responsabilidad social corporativa indicando que la segunda es una de las dimensiones de la primera. Mientras que la ética corporativa abarca los lineamientos de valores y buenas prácticas en cada ámbito de aplicación, la responsabilidad social corporativa debe asumirse como "herramienta de gestión, medida de prudencia y exigencia de justicia"[80].

Con respecto a la responsabilidad social corporativa, Lokke Moerel explica que típicamente se la aplica en el ámbito del respeto a los derechos humanos, la protección del medio ambiente, oposición al soborno y corrupción, al compromiso de ser justos con clientes y proveedores. No obstante, estos ámbitos están en constante expansión. Ahora también, se incluye el compromiso de las empresas de proteger los datos personales[81].

La cultura de ética empresarial no es muy arraigada en el Ecuador. De hecho, el pensamiento generalizado de muchas personas, según Francisco Santamaría, es que supone más costos que beneficios [82]. No se le da suficiente importancia a la responsabilidad ética corporativa, cuando en realidad, se debería incentivar a la inversión en adopción de programas de cumplimiento integral, incluyendo en la protección de datos.

En concreto, ¿qué beneficios brinda la cultura ética empresarial y responsabilidad social corporativa en materia de protección de datos? Primero, evitar las sanciones pecuniarias por infracciones a la normativa. La sanción por infracciones graves en la LOPDP va del 0.7% al 1% calculados sobre el volumen de negocios de la entidad[83]. Si las empresas fortalecen internamente una cultura ética de cumplimiento de las reglas de protección de datos, no experimentarán detrimento en sus economías por multas.

Un segundo beneficio es mejorar la competitividad en el mercado nacional e internacional. Alinearse a las buenas prácticas corporativas envía un mensaje positivo de

[80] Adela Cortina, "Ética de La Empresa: no sólo responsabilidad social.", *Revista Portuguesa de Filosofia* 65, núm. 1/4 (2009), 113–27.
[81] Lokke Moerel, *Binding Corporate Rules. Corporate self-regulation of global data transfer*.
[82] José Francisco Santamaría Ramos, "El principio de responsabilidad proactiva".
[83] Artículo 72, LOPDP.

confianza externamente. Si entidades internacionales, exigentes en la protección de datos personales, ponen su mirada en este país en busca de acuerdos comerciales, van a tener preferencia a aquellas empresas que cumplan con garantías de protección de los datos personales de sus clientes. Entonces, esa confianza se traduce a beneficios económicos, como indica Adela Cortina, porque supondría una reducción en costos de coordinación a nivel interno y externo[84]. No se debe olvidar que la UE es uno de los principales aliados comerciales, con el que se ha firmado varios acuerdos bilaterales[85].

Muy importante es el beneficio de la reputación empresarial. Una buena reputación atrae a accionistas, trabajadores, clientes, proveedores, etc., generando más valor a dicha empresa. El valor de una empresa, o *enterprise value,* se mide en función de sus activos tangibles e intangibles[86]. Las bases de datos son parte de los activos intangibles, de modo que, si una empresa es sancionada o está en riesgo de ser sancionada por vulnerar información, reduce gravemente su valor.

Los usuarios también tienen influencia en la valoración de una empresa, cuando escogen aquellas comprometidas con la protección de sus datos personales elevan el perfil de dicha empresa en el mercado. Por eso, el cumplimiento normativo de protección de datos "no solo comporta el beneficio de evitar sanciones, sino también beneficios para la imagen y reputación corporativa, ayuda a minimizar riesgos y optimiza recursos económicos"[87]

8. Conclusiones

Ecuador está construyendo un sistema jurídico de protección de datos personales con base en el modelo europeo. En el régimen de transferencia internacional de datos, la LOPDP pretende incluir los mismos estándares del RGPD. El primer estándar se refiere a la regla general de que el país receptor cuente con un nivel adecuado de protección mediante decisión de adecuación. El segundo estándar es la existencia de garantías adecuadas, como códigos de conducta, a falta de decisión de adecuación.

[84] Adela Cortina, "Ética de La Empresa: no sólo responsabilidad social."
[85] Delegation of the European Union to Ecuador, "Comercio bilateral entre la Unión Europea y Ecuador creció un 16% en 2021", Institucional, EEAS Website, el 2 de febrero de 2022, https://www.eeas.europa.eu/delegations/ecuador/comercio-bilateral-entre-la-uni%C3%B3n-europea-y-ecuador-creci%C3%B3-un-16-en-2021_en?s=161.
[86] Luis Alberto Montezuma Chávez y Qian Li Loke, "Privacy Compliance Matters to a Company's Valuation", *The International Association of Privacy Professionals* (blog), de agosto de de 2018, https://iapp.org/news/a/privacy-compliance-matters-to-a-companys-valuation/, (último acceso: 18/11/2022).
[87] José Francisco Santamaría Ramos, "El principio de responsabilidad proactiva".

Excepcionalmente, según el tercer estándar, se puede aceptar una transferencia de datos en situaciones específicas que son taxativas.

A pesar de las similitudes de los estándares en ambos sistemas, la LOPDP no logra satisfacer los requerimientos para que Ecuador sea considerado un país seguro para la transferencia internacional de datos. En concreto, esta ley no recoge las regulaciones con respecto a las transferencias ulteriores, ni tampoco brinda definiciones claras de términos como 'nivel adecuado de protección' o 'normas corporativas vinculantes'. Adicionalmente, aún no se ha promulgado un reglamento a la ley y aún se está configurando la Superintendencia de Protección de Datos. Todo esto dificulta el proceso para obtener una resolución de adecuación positiva de CE.

Por este motivo, en el sector empresarial se debe fortalecer la autorregulación mediante normas corporativas vinculantes y códigos de conducta como mecanismos que demuestran una actitud proactiva y demostrada en el cumplimiento de la normativa. El principio de responsabilidad proactiva es la columna vertebral del sistema de protección de datos personales porque demanda que los responsables y encargados no se conformen con el mero cumplimiento normativo, sino que demuestren iniciativa y debida diligencia en todo momento.

A través de las normas corporativas vinculantes que se adopten dentro de un grupo o unión empresarial, bastaría la aprobación de una de las autoridades de control que se encuentre en territorio con nivel adecuado de protección para que la entidad ecuatoriana quede bajo dicho sistema jurídico de forma indirecta y que la transferencia de datos personales se realice libremente. Los códigos de conducta, por su parte, pueden ser útiles, como atenuantes de responsabilidad civil y penal, e incluso, se discute a nivel doctrinario la posibilidad de servir como eximentes de responsabilidad penal a través de un adecuado esquema de autorregulación.

En todo caso, el recorrido que está haciendo el país en este nuevo sistema de protección de datos recalca la necesidad de incentivar la cultura ética y responsabilidad social en el seno de las empresas. Sobre todo, porque los beneficios que puede traer incluyen: evitar sanciones pecuniarias impuestas por la autoridad de protección, tener más competitividad en los mercados nacional e internacional, generar confianza y buena reputación ante inversores, clientes, trabajadores, accionistas, etc.

Como recomendaciones en los próximos pasos hacia el perfeccionamiento del sistema ecuatoriano, primero, el reglamento a la LOPDP debe ser flexible en permitir a las empresas ecuatorianas interesadas adherirse a normas corporativas vinculantes

aprobadas por una autoridad de un país con un nivel de protección de datos mayor al del Ecuador. Con dicha aprobación, debería entenderse que han sido aceptadas también a nivel local. Esto tiene concordancia con lo que estipulado en el literal a) de la LOPDP. También, se debe ampliar la posibilidad de los códigos de conducta como eximentes de responsabilidad.

Luego, el futuro Superintendente de Protección de Datos debe direccionar sus actuaciones a reforzar los estándares de transferencia de datos en el Ecuador y completar con normativa secundaria lo que está faltando en la LOPDP. También, los administradores de justicia tienen un rol fundamental en la interpretación de ley en los casos concretos de responsabilidad de las instituciones. En específico, deberán. observar la línea jurisprudencial del TJUE, tomando en cuenta que es el modelo seguido por la Ley.

Finalmente, el sector empresarial ecuatoriano debe buscar asociarse con aquellas entidades que se encuentran en países catalogados con nivel adecuado de protección; así como fomentar la cultura de ética y responsabilidad social empresarial a través de la implementación de mecanismos de autorregulación.