CENTRO
LATAM
DIGITAL

Políticas de **Competencia** y **Protección de Datos Personales**

Perspectivas para América Latina

Políticas de **Competencia** y **Protección de Datos Personales**

Perspectivas para América Latina[1]

María Solange Maqueo[2] y María Fernanda Viecens[3]

1. Las autoras agradecen los comentarios recibidos de los participantes de la Mesa debate: Políticas de Competencia, Privacidad y Uso de datos de CPR LATAM del 25 de octubre 2021, en particular, de Isaac Alcalá, Victor Fernandes y Carlos Lugo Silva.

2. María Solange Maqueo (PhD en Derecho) es Directora de la División de Estudios Jurídicos del Centro de Investigación y Docencia Económicas (CIDE). Ha sido consultora externa de organismos internacionales entre los que se encuentra el Consejo de Europa. Fue Consejera Presidenta del Consejo Consultivo del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

3. María Fernanda Viecens (PhD en Economía) es investigadora CONICET en el Centro Tecnología y Sociedad (CETyS) de la Universidad de San Andrés. Ha sido Vocal de la Comisión Nacional de Defensa de la Competencia (CNDC). Es profesora de la Universidad de San Andrés y de la Universidad Torcuato Di Tella.

Centro Latam Digital 2022
Primera edición: Julio de 2022

Para más información sobre las publicaciones y proyectos de Centro Latam Digital, visite nuestro sitio web centrolatam.digital.

Este trabajo se llevó a cabo con una subvención del Centro Internacional de Investigaciones para el Desarrollo (IDRC), Ottawa, Canadá. Las opiniones expresadas en este documento no representan necesariamente las del IDRC o su consejo superior

Diseño de tapa y diagramación:
Elisabet Lunazzi

IDRC · CRDI
International Development Research Centre
Centre de recherches pour le développement international

Canada

Abstract

Uno de los elementos que caracteriza la transformación digital es la generación y uso de cantidades crecientes de datos de consumidores. Todo este potencial será sostenible si la competencia funciona correctamente en los mercados digitales y, además, se protegen los derechos y privacidad de los ciudadanos. El objetivo de este trabajo es contribuir a la identificación y comprensión de las mejores políticas públicas que interaccionan en la economía digital. Para esto, el artículo analiza los diferentes enfoques bajo los cuales interactúan las políticas de competencia y protección de datos personales, y la evidencia existente en la región sobre esta interacción. Se revisan, también, las herramientas disponibles en las agencias de América Latina, con el objetivo final de proponer un conjunto de factores que deberían ser útiles como guía para la discusión.

Índice

Resumen ejecutivo

Uno de los elementos que caracteriza la transformación digital es la generación y uso de cantidades crecientes de datos de consumidores. Esto está impulsado principalmente por nuevos modelos comerciales de plataformas digitales que se basan en la recopilación y procesamiento de datos de los consumidores para diferentes fines. Sin embargo, todo este potencial será sostenible si la competencia funciona correctamente en los mercados digitales y se protegen los derechos y privacidad de los ciudadanos. La pandemia Covid 19 ha sumado presión sobre las políticas públicas relacionadas con la economía digital y los enfoques regulatorios deben interoperar constantemente para promover un ecosistema digital con todos los beneficios para los usuarios y la sociedad.

El objetivo de este trabajo es contribuir a la identificación y comprensión de las mejores políticas públicas que interaccionan en la economía digital. Para ello, este artículo identifica los diversos enfoques existentes respecto de la interacción entre la política de competencia económica y la protección de datos personales. En un primer enfoque, ambas políticas tienen un tratamiento normativo independiente, con objetivos diferenciados. Un segundo enfoque atiende a la privacidad como medida afectada por la competencia. Esto es, la afectación de la privacidad o la protección de datos personales puede considerarse como un efecto de potenciales prácticas anticompetitivas, o bien, como un aspecto que debe ser considerado durante el análisis para el control preventivo en las concentraciones. Un tercer enfoque, por su parte, atiende a las posibles tensiones entre las legislaciones en materia de competencia económica y la privacidad y protección de datos personales, por ejemplo, cuando una y otra legislación rivalizan en cuanto a la apertura o la confidencialidad de la información. Finalmente, un cuarto enfoque hace referencia a los costos anticompetitivos que pudiera llegar a suponer una regulación estricta en materia de privacidad y protección de datos personales. Este supuesto hace referencia al costo de cumplimiento de esta legislación como una potencial barrera de entrada al mercado.

Asimismo, en este artículo se abordan, desde una perspectiva regional, los distintos enfoques en los que interactúa la política de competencia económica con la privacidad y la protección de datos personales para contribuir al objetivo de identificar y comprender las mejores políticas públicas para la economía digital de la región. Para esos efectos, se incorporan casos y evidencia que permiten ejemplificar aquellos supuestos en los cuales se incorporan cuestiones relacionadas con la privacidad y la protección de datos personales en el análisis de la política de competencia económica.

Por otra parte, este artículo comprende un análisis de estándares internacionales en materia de privacidad y protección de datos personales, a fin de identificar distintos niveles de exigencia, en contraste con el Reglamento General de Protección de Datos de la Unión Europea (RGPD). Este estudio parte del supuesto de que este ordenamiento supone el nivel más elevado de exigencia.

Con base en los indicadores seleccionados del RGPD, se analiza la legislación vigente de Argentina, Brasil, Chile, Colombia, El Salvador, México y Perú, en materia de privacidad y protección de datos personales, con el objeto de identificar su cercanía o distanciamiento con el modelo regulatorio de la Unión Europea. Este análisis comparativo nos permite observar que México es el país que mayor influencia ha recibido a partir de este Reglamento, especialmente por lo que hace a su legislación aplicable para el sector público. Por su parte, El Salvador es el país que presenta más diferencias, dado su modelo

regulatorio sectorial en la materia. Estos hallazgos son consistentes con los distintos niveles de exigencia de los instrumentos internacionales, toda vez que la elaboración de los Estándares Iberoamericanos de Protección de Datos Personales se llevó a cabo durante la presidencia de México en la Red Iberoamericana de Protección de Datos.

Después de realizar el análisis comparado, a partir de la previa selección de indicadores relativos a los principios, obligaciones y el régimen aplicable a las categorías especiales de datos, se concluye que los Estándares Iberoamericanos de Protección de Datos Personales, elaborado por la Red Iberoamericana de Protección de Datos, es el que mayor cercanía presenta con el RGPD. Este hallazgo resulta significativo si consideramos que este instrumento internacional de *soft law* pretende guiar el diseño normativo de la protección de datos personales en los países de la región, con el objeto de generar estándares comunes.

Introducción

Uno de los elementos que caracteriza la transformación digital es la generación y uso de cantidades crecientes de datos de consumidores. Esto está impulsado principalmente por nuevos modelos comerciales de plataformas digitales que se basan en la recopilación y procesamiento de datos de los consumidores para diferentes fines, como mejorar los servicios publicitarios de donde provienen los ingresos. Sin embargo, todo este potencial será sostenible si la competencia funciona correctamente en los mercados digitales y se protegen los derechos y privacidad de los ciudadanos. La pandemia Covid 19 ha sumado presión sobre las políticas públicas relacionadas con la economía digital y los enfoques regulatorios deben interoperar constantemente para promover un ecosistema con todos los beneficios para los usuarios y la sociedad. El objetivo de este trabajo es contribuir a la comprensión de las mejores políticas públicas que interaccionan en la economía digital.

Los datos personales se han convertido en objeto de comercio en la economía digital y las empresas compiten para adquirir y procesar estos datos (Costa-Cabral & Lynskey, 2017). En este contexto se observa una tendencia creciente a nivel global de interés por elevar los estándares de protección de datos personales y propiciar la modernización de los instrumentos pioneros en la materia, así como la aprobación de nuevas legislaciones que sustituyen a las ya existentes o que incorporan, por primera vez, un régimen de protección de datos personales en su derecho interno. En Europa en particular, entró en vigor el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo en abril de 2016 conocido como el Reglamento General de Protección de Datos (RGPD) que está actuando como referencia para legislaciones y discusiones parlamentarias en la región.

Asimismo, si bien la política de competencia y la de privacidad de datos se rigen por diferentes textos legales y su aplicación es supervisada por diferentes autoridades con diferentes mandatos, la interacción entre ambas legislaciones ha mostrado cierta evolución en el tiempo, como así también diferentes voces en relación con cómo debe implementarse dicha interacción. En 2014, en la fusión Facebook-Whatsapp la Comisión Europea estableció una taxativa separación en el alcance de ambas legislaciones, donde señaló: *Cualquier preocupación relacionada con la privacidad que surja de la mayor concentración de datos bajo el control de Facebook como resultado de la transacción no cae dentro del alcance de las reglas de la ley de competencia de la UE, sino dentro del alcance de las reglas de protección de datos de la UE* (traducción de las autoras).[4] Pocos años después, en 2019, el *Bundeskartellamt*, en un caso con mucha repercusión en el ámbito de la política de competencia, llevó a cabo una investigación en contra de Facebook por abuso explotativo donde la privacidad es tratada como medida afectada por la competencia. En mayo 2021, la agencia de competencia de Argentina inició una investigación contra Facebook-Whatsapp por una posible conducta anticompetitiva y ordenó una suspensión preventiva de la actualización de los Términos de servicio y la Política de privacidad de Whatsapp.[5] La medida fue extendida en marzo 2022 y confirmada en abril 2022 por la Justicia. En Brasil,

4. Facebook-Whatsapp merger European Commission https://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf. Una posición similar ya había mostrado la Comisión en 2008 en la fusión Google/Doubleclick de 2008 (Case No COMP/M.4731 – Google/ DoubleClick): ...La presente Decisión se entiende sin perjuicio de las obligaciones impuestas a las partes por la legislación comunitaria en relación con la protección de las personas y la protección de la intimidad en lo que respecta al tratamiento de datos personales... (traducción de las autoras).

5. https://www.argentina.gob.ar/noticias/comercio-interior-dicto-una-medida-cautelar-contra-facebook-para-evitar-que-whatsapp-0

por su parte,se llevó a cabo una recomendación conjunta del *Conselho Administrativo de Defesa Económica* (CADE), el *Ministerio Público Fiscal* (MPF), la *Autoridade Nacional de Proteção de Dados* (ANPD), y la *Secretaria Nacional do Consumidor* (Senacon) con los mismos fines.[6]

Como parte de estos acontecimientos, se ha desarrollado en los últimos años una creciente literatura sobre la interacción entre los datos, la política de privacidad y la ley de competencia a nivel académico y de políticas públicas. La OCDE, por su parte, está impulsando un debate informado sobre los derechos de los consumidores en relación con el uso de sus datos, la economía digital y la competencia (OCDE, 2016; OCDE, 2020a). Destacan también las especificidades normativas de cada jurisdicción, con diferencias importantes.[7]

Teniendo en cuenta estos antecedentes, este artículo analiza los diferentes enfoques bajo los cuales interactúan las dos políticas (competencia y privacidad), revisa las herramientas disponibles en algunas agencias de América Latina, para finalmente proponer un conjunto de factores que deberían ser útiles como guía para la discusión en los países de la región. En particular, se lleva a cabo un análisis de estándares internacionales en materia de privacidad y protección de datos personales, a fin de identificar distintos niveles de exigencia, en contraste con el Reglamento General de Protección de Datos de la Unión Europea (RGPD), con el supuesto de que este ordenamiento representa el nivel más elevado de exigencia. Con base en un conjunto de indicadores seleccionados del RGPD, se analiza la legislación vigente de Argentina, Brasil, Chile, Colombia, El Salvador, México y Perú, en materia de privacidad y protección de datos personales, con el objeto de identificar su cercanía o distanciamiento con el modelo regulatorio de la Unión Europea.

La siguiente sección identifica cuatro enfoques de interacción entre las dos políticas que se deducen de la literatura y casos de defensa de la competencia. La sección tres analiza los enfoques desde la perspectiva regional. La sección cuatro describe los diferentes estándares de las legislaciones de competencia a nivel global, para luego reconocer los correspondientes en las legislaciones de los países de América Latina. La Sección 5 presenta las principales conclusiones del estudio.

6. https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/recomendacao_whatsapp_-_assinada.pdf

7. Por ejemplo, Liguori et al (2021) analizan la temática con perspectiva europea y Marthews & Tucker (2019). hacen lo mismo para EE. UU.

2. Enfoques sobre la interacción entre las políticas de competencia y protección de datos

La legislación de competencia aplica a toda actividad económica. En particular, la legislación de protección de datos aplica a la actividad de procesamiento de datos personales, ya sea en una actividad económica como en actividades que no son económicas. La tabla a continuación resume los enfoques identificados en la literatura y decisiones públicas de las agencias sobre la interrelación entre estas dos legislaciones. Luego, se analiza en detalle cada uno de los mismos. Si bien algunos enfoques son contrapuestos, otros son complementarios y un análisis de política pública amerita recorrer una evaluación de todos.

Legislaciones independientes	Privacidad como medida afectada por la competencia	Legislaciones en tensión	Legislación de privacidad como costo anticompetitivo
La política de competencia debe tener como único objetivo la promoción de la competencia.	Efectos sobre protección de datos y privacidad incluidos en la evaluación de una práctica potencialmente anticompetitiva y del control preventivo de fusiones. Privacidad asemejada a calidad Legislación de privacidad como estándar	Privacidad como defensa para potenciales prácticas anticompetitivas (ej., negar acceso a datos). Los remedios de acceso de datos que se plantean desde competencia y como regulación ex – ante podrían vulnerar la legislación de privacidad.	Costos de legislaciones estrictas (GDPR) Efectos anticompetitivos de la legislación de privacidad

Tabla 1. Enfoques para la interacción competencia-protección de datos

2.1 Legislaciones independientes

En decisiones relativamente recientes, la Comisión Europea sostuvo que las cuestiones relativas a la protección de datos derivadas de las fusiones caían fuera del ámbito de la legislación de competencia y debían ser contempladas bajo el paraguas de la legislación de protección de datos. De acuerdo con este enfoque, la política de competencia debe tener como único objetivo la promoción de la competencia y no es su tarea la protección de datos y la privacidad en general. Desde este punto de vista la legislación actual sobre privacidad y protección del consumidor, este criterio es suficiente para atender estas preocupaciones. Sin embargo, una preocupación de quienes apoyan esta perspectiva es que la incorporación de consideraciones de privacidad en el análisis de competencia creará confusión en la aplicación del estándar de bienestar del consumidor (Douglas, 2021).

2.2. Privacidad como medida afectada por la competencia

El fin último de la legislación de competencia es la protección del interés económico general frente a acciones potencialmente anticompetitivas de las empresas que actúan en los mercados. Tradicionalmente, el estándar de análisis considerado para el interés económico general ha sido el impacto sobre los precios y las cantidades comercializadas en el mercado.

Asimismo, el impacto sobre la calidad de los productos y servicios transaccionados también ha sido incluido en el análisis. Recientemente, a raíz de una serie de fusiones globales en el sector de semillas y agroquímicos, la Comisión Europea introdujo explícitamente consideraciones sobre el impacto de las operaciones en la innovación de la industria.[8] En el contexto del uso de datos en la economía digital, el análisis de competencia ha empezado a incorporar el análisis de la afectación a la privacidad de los usuarios de servicios como resultado de adquisiciones o abuso de posición dominante (tipo explotativo). Esto implica incluir la protección de datos en el análisis de competencia, entendiendo que el nivel de protección de datos ofrecido a los particulares está sujeto a competencia. Por lo tanto, los aspectos de las leyes de protección de datos como las condiciones que rigen el procesamiento de datos personales sensibles, pueden ser parámetros de competencia y la ley de protección de datos puede ayudar a la ley de competencia a juzgar su alcance (Costa-Cabral & Lynskey, 2017).

Esto puede ser entendido como una manera amplia de interpretar la calidad. Bajo este enfoque se considera si las fusiones o conductas reducen las opciones disponibles de privacidad para los consumidores (ya que se asume que las empresas compiten en el nivel de privacidad que ofrecen).

Consistente con este enfoque, en 2019 el *Bundeskartellamt*, en un caso con mucha repercusión en el ámbito de la política de competencia, llevó a cabo una investigación en contra de Facebook por abuso explotativo donde la privacidad aparece como la medida afectada por la competencia.[9] Las actuaciones recientes en Argentina y Brasil mencionadas en la introducción y explicadas con más detalle en la siguiente sección, se han desarrollado también en este marco.

Bajo esta perspectiva, la ley de protección de datos proporciona la orientación normativa en relación con un parámetro competitivo distinto de los precios, como es la privacidad y las condiciones de protección de datos y este fue precisamente el estándar adoptado por el *Bundeskartellamt* en el caso Facebook. De esta manera, infracciones de la ley de protección de datos o cambios perjudiciales en la protección de datos, pueden indicar explotación del consumidor o presencia de prácticas anticompetitivas. Nótese que, tal como Costa-Cabral & Lynskey (2017) señalan, tal uso de la ley de protección de datos como un punto de referencia normativo no expande la noción de bienestar del consumidor tal como se viene entendiendo, sino que proporciona un estándar para determinar la existencia, o no, de conducta.

Con este enfoque, las consideraciones de privacidad afectan las revisiones de fusiones y eventualmente la decisión de autorizar o bloquear una fusión. De hecho, uno de los primeros casos donde se mencionan consideraciones sobre la privacidad fue en la fusión de Google / DoubleClick, en la FTC de EE. UU.[10] En TomTom / TeleAtlas, la Comisión analizó el riesgo de que la acumulación de datos pudiera llevar a una reducción del nivel de protección de los datos confidenciales. Microsoft / LinkedIn es también un precedente relevante en la

8. Véanse casos Dow-Dupont y Bayer-Monsanto.

9. https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=5.

10. Aunque se señaló que el único propósito de la revisión antimonopolio federal de fusiones y adquisiciones es identificar y remediar transacciones que dañan la competencia (https://www.ftc.gov/news-events/press-releases/2007/12/federal-trade-commission-closes-googledoubleclick-investigation).

evaluación de la Comisión de fusiones que involucran cuestiones relacionadas con datos en industrias tecnológicas y conglomerados digitales.[11]

Para la fusión Facebook-Whatsapp, Costa-Cabral & Lynskey (2017) cuestionan que, a pesar de que se reconoció la importancia de la protección de datos para los consumidores, la Comisión no consideró los efectos de la competencia en la protección de datos, es decir, si por ejemplo Facebook podía alterar las condiciones de protección de datos de WhatsApp en detrimento del consumidor como resultado de la operación.

Finalmente, el proyecto de la Digital Market Act señala "*The data protection and privacy interests of end users are relevant to any assessment of potential negative effects of the observed practice of gatekeepers to collect and accumulate large amounts of data from end users*". El Proyecto refiere a prácticas de los denominados Gatekeepers, con una perspectiva de tratamiento de datos afectado por la competencia.

2.3 Legislaciones en tensión

Douglas (2021) sostiene que las dos legislaciones deberían interactuar como sucede con las de competencia y propiedad intelectual, por ejemplo. Al respecto, la autora identifica dos tensiones.

La primera tensión identificada es el uso de la legislación de protección de datos como justificación/explicación de potenciales prácticas que de otra manera serían anticompetitivas. Por ejemplo, en Europa las empresas se justifican en la GDPR para no dar acceso a los datos. En USA, las plataformas digitales invocan privacidad de datos como defensa frente a denuncias por prácticas anticompetitivas. Al respecto, la Sherman Act establece que si existe una justificación para la práctica, el denunciado escapa de la responsabilidad de la misma. Entonces, Douglas (2021) señala que así como en el pasado la justificación se ofrecía muchas veces por defensa del consumidor y propiedad intelectual, ahora se hace por privacidad. Sin embargo, ella señala que en el enforcement de antitrust no se está reconociendo como tal (como sí se hace con defensa del consumidor y propiedad intelectual). En este sentido, Douglas (2021) plantea que la atención a la competencia "le está ganando" a la atención por privacidad.

La segunda tensión identificada es que los remedios de acceso de datos que se plantean desde competencia y como regulación *ex–ante* podrían vulnerar la legislación de competencia. La capacidad de transferir datos, conocida como portabilidad de los datos, ha adquirido protagonismo en la discusión sobre plataformas y competencia en la economía digital. Asimismo, remedios que obligaban a acceso de datos han sido usados históricamente, como en el caso Microsoft en el que se obligó a dar acceso a la información de las interfaces. Estos remedios surgen frente a una preocupación por la gran ventaja competitiva que los datos pueden conferir.[12] Sin embargo, los remedios que se discuten tienen un impacto potencial en la privacidad. Si bien el acceso a dichos datos es necesario para restaurar la competencia con las plataformas digitales, ese acceso bien puede erosionar la privacidad de los consumidores. Las tensiones entre legislaciones

11. Case M.8124 – Microsoft / LinkedIn, https://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf

12. Tucker (2020) es crítica con el argumento de que los datos generan un potencial exclusorio para las empresas que los poseen. Ella sostiene que si bien las empresas podrían controlar el acceso a una base de datos en particular, no pueden controlar la capacidad de las competidoras de crear otra base de datos similar. En particular, no pueden controlar la capacidad de una empresa rival para crear un conjunto de datos que ofrezca información similar.

surgen porque mientras que con el acceso a los datos la competencia puede mejorar, la privacidad de los datos puede resultar erosionada.

Douglas (2021) contrapone este enfoque con el de "privacidad como medida competitiva". Al respecto, la autora argumenta que la legislación de privacidad debe interactuar con la de competencia de manera separada y potencialmente opuesta, y no ser la privacidad un mero factor dentro del análisis de *antitrust*. Asimismo, sostiene que la aplicación de la legislación *antitrust* no estaría considerando a la legislación de privacidad en igualdad de condiciones y propone que se la ponga a la altura, como se ha resuelto anteriormente con tensiones análogas que surgieron en su momento con la legislación de propiedad intelectual y la de defensa del consumidor.

2.4 Legislación de privacidad como costo anticompetitivo

Gal & Aviv (2020) cuestionan el RGPD como una regulación costosa que daña la competencia y la innovación. Los autores sostienen que estos efectos negativos sobre la competencia y la innovación justificarían una reevaluación del equilibrio existente. Más precisamente, los autores señalan que el RGPD europeo ha generado una serie de preocupaciones y estudios en relación con un potencial impacto anticompetitivo de la normativa. Ellos sostienen que el costo del cumplimiento del Reglamento es tan alto que se traduce en una ventaja para las grandes empresas (las '*BigTech*'), lo que además aumenta la concentración de los datos y fortalece a quienes los poseen. Esto lleva también a que, dada la integración vertical de algunas BigTech en el mercado de publicidad online, se posicionan con una fuerte ventaja frente a competidores más pequeños y no integrados verticalmente. De esta manera, Gal & Aviv (2020) sostienen que el RGPD limita la competencia, fomenta la concentración de datos y de los mercados vinculados a los datos, mientras que potencialmente fortalece a las grandes empresas que controlan datos.

Marthews & Tucker (2019), por su parte, sostienen que existe un *tradeoff* entre promover la competencia y proteger la privacidad de los usuarios, análogo a los que se generan también entre la competencia con la innovación y la protección medioambiental. Muestran evidencia que sugiere que el costo del RGPD por empleado es proporcionalmente mayor para las empresas pequeñas. Además, argumentan que la necesidad de consentimiento de los usuarios podría implicar barreras a la entrada de nuevas firmas ya que los consumidores tienen más probabilidades de dar su consentimiento para que sus datos sean procesados por empresas con las que ya tienen relación. Asimismo, los paquetes de productos podrían exacerbar esta desventaja. El RGPD sugiere que una empresa debe lograr el cumplimiento de la privacidad con cada socio que procesa los datos de los visitantes del sitio que se utilizan en la publicidad dirigida. En este caso, un servicio integrado verticalmente como el de Google AdSense, que permite verificar el cumplimiento con un único socio publicitario presenta enormes ventajas frente a operadores más pequeños no integrados verticalmente. Al mismo tiempo, los autores muestran casos que evidencian que los consumidores no valoran o valoran muy poco la privacidad. En particular, ellos plantean lo que se conoce como la "paradoja de la privacidad". Esto es, mientras que los usuarios expresan preocupación por la privacidad, no actúan en consecuencia con dicha preocupación (Athey, Catalini & Tucker, 2017). Consistente con este argumento, en OCDE (2020b) se señala que las políticas de privacidad, y su eventual empaquetamiento, pueden crear barreras de entrada para nuevas empresas. En particular, para poder competir estas nuevas empresas deben ingresar simultáneamente en numerosos mercados y comprar datos costosos para replicar las ventajas de los conglomerados digitales.

3. Los enfoques en perspectiva regional

Mientras que la anterior sección definió y revisó los enfoques en función de antecedentes internacionales, esta sección revisa la experiencia regional existente para cada enfoque.

3.1 Antecedentes sobre interpretación de legislaciones independientes

En Brasil, durante el año 2021 Serasa (empresa de servicios de información) y Claro (empresa de telecomunicaciones) notificaron en CADE un contrato de prestación de servicios por el cual Claro proveería datos de los usuarios de sus servicios que Serasa usaría como insumo de sus soluciones para protección de créditos y prevención de fraudes. CADE descartó preocupaciones por efectos exclusorios anticompetitivos como resultado del acuerdo y además señaló:

"*...Cade no se responsabiliza de analizar si el contrato bajo análisis y las respectivas cláusulas de exclusividad están de acuerdo o no con la Ley General de Protección de Datos Personales (Ley N ° 13.709 / 2018), la Ley de Registro Positivo (Ley N ° 12.414) o Decreto No 9936/2019. La aprobación de la operación por parte de Cade se refiere únicamente al tema de competencia, y no implica un análisis de fondo en cuanto a si los Postulantes se adhieren o no a la normativa antes mencionada, cuya inspección de cumplimiento es responsabilidad de las respectivas autoridades gubernamentales*".[13]

Si bien CADE en esta decisión muestra cierta evidencia en línea con el enfoque de legislaciones independientes, no se puede inferir de esta cita una postura concluyente de la agencia sobre la interacción de las legislaciones, ya que la misma se aplica en una situación y caso específicos.

3.2 Casos donde la privacidad es incorporada en la evaluación de los efectos competitivos de una conducta o fusión.

Los reguladores de la región siguen de cerca la discusión internacional y están comenzando a tomar medidas. En mayo de 2021, la agencia de competencia de Argentina inició una investigación contra Facebook por una posible conducta anticompetitiva y ordenó una suspensión preventiva de la actualización de los Términos de servicio y la Política de privacidad de WhatsApp. Como el caso del Bundeskartellamt en Alemania, el intercambio de datos entre diferentes servicios de la empresa (Facebook y Whatsapp) está en el corazón de las teorías del daño argumentadas por la agencia.[14] En Brasil se llevó a cabo

13. Véase Ato de Concentração nº 08700.006373/2020-61.

14. El presidente de la agencia y representante de la empresa estuvieron presentando y explicando el caso en el Congreso argentino.

una recomendación conjunta que desarrolla una preocupación similar. Ambos casos se encuadran en el enfoque de privacidad como medida competitiva. Por su parte, la nueva Guía de la Fiscalía Nacional Económica (FNE) de Chile para el análisis de operaciones de concentración horizontales de mayo 2020 señalan que:

"La Fiscalía analizará con detención los posibles efectos de la Operación tomando en consideración no sólo su dimensión horizontal, sino que también aspectos verticales y/o de conglomerado. Respecto a los aspectos horizontales, la Fiscalía analizará con mayor detención los efectos competitivos en los mercados que concurran los siguientes elementos, no taxativos." (FNE, 2021: 34).
ii. Cuando se puedan generar riesgos de menoscabo de variables distintas al precio, tales como términos de uso de las plataformas (ej. políticas de privacidad) y los incentivos a innovar de las partes que se concentran;"

Además, en la fusión Uber-Cornershop, la FNE analiza (y descarta) riesgos de efectos explotativos de la operación "*Derivados principalmente de una eventual imposición a los consumidores finales de políticas de privacidad más gravosas*".[15] El informe de aprobación menciona en dos ocasiones a la Ley 19.628 sobre protección de datos de carácter personal. Es interesante mencionar como antecedente el bloqueo por parte de la FNE en 2004 de la fusión Falabella/D&S donde la tenencia de datos ocupó un elemento relevante en el análisis (Facuse, 2021).

En 2018 Cofece elaboró un documento que revisa y evalúa los desafíos de la economía digital (Cofece, 2018). El informe señala como posibilidad el incorporar la privacidad como variable afectada por la competencia.

3.3 Evidencia sobre legislaciones en tensión

Las interacciones observadas que encuadran dentro de este enfoque han sido variadas y en diferentes sectores de la economía. La Superintendencia de El Salvador recibió un pedido de opinión del Congreso durante el tratamiento del proyecto de la Ley de protección contra el tratamiento indebido de datos personales. En respuesta, la Superintendencia opinó sobre la importancia de las figuras de la portabilidad de datos personales y la transferencia de datos para reducir barreras de entrada y propiciar escenarios favorables para la libre competencia en los mercados. Esta recomendación encuadra dentro del enfoque de legislaciones en tensión, ya que la Superintendencia como resultado de la revisión del proyecto de la legislación de tratamiento de datos realiza comentarios tendientes a favorecer la competencia pero que podrían eventualmente colisionar con el objetivo de dicha legislación.[16]

La SIC de Colombia, en su rol de abogacía de la competencia, ha emitido una serie de recomendaciones tendientes a reducir costos de cambio y por ende promover la competencia, en sectores de telecomunicaciones (portabilidad), a la normativa de facturación digital, y otras recomendaciones regulatorias que de alguna manera afectaban el tratamiento de datos (OCDE-Colombia, 2020). Estas iniciativas por parte de la agencia

15. Informe de Aprobación Uber-Cornershop de la FNE, https://www.fne.gob.cl/wp-content/uploads/2020/06/inap2_F217_2020.pdf.

16. https://www.sc.gob.sv/index.php/sala_multimedia/opinion-normativa-proyecto-ley-de-proteccion-contra-el-tratamiento-indebido-de-datos-personales-sc-039-s-on-nr-2019/

de competencia se enmarcan dentro de la tensión que puede surgir entre la protección de los datos y la protección de la competencia. De manera análoga, en México la Ley Federal de Telecomunicaciones y Radiodifusión impone al operador preponderante de telecomunicaciones una serie de obligaciones en materia de datos e información, a los fines de generar condiciones competitivas, siempre en cumplimiento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (véase OECD-México, 2020). Una mención particular merece el caso Bradesco-Guiabolsa en CADE Brasil, que actuó como precedente del open-banking en ese país. Guiabolsa es una Fintech que para prestar sus servicios requería contar con los datos de los usuarios (con los correspondientes consentimientos) en las instituciones financieras donde son clientes. La investigación inició en 2018 a raíz de una práctica de Bradesco de solicitar una contraseña adicional cuando los clientes querían insertar sus datos en la plataforma de Guiabolso. Esto fue interpretado por CADE como una potencial práctica anticompetitiva de negativa de acceso. En octubre de 2020 se homologó un Compromiso de Cese por el cual Bradesco se comprometió a interrumpir la conducta investigada y pagar una multa.[17]

Contrario a los casos analizados bajo la perspectiva de este enfoque, la fusión Magalu-Hub en CADE muestra un caso donde la legislación de protección de datos es aprovechada por la agencia de competencia para eliminar preocupaciones competitivas.[18] En este caso, habiendo sido aprobada la operación por CADE, Mercado Pago como tercero interesado presentó un recurso señalando que la operación implicaba que un competidor accedería a datos sensibles de Mercado Pago, lo que le otorgaba ventajas competitivas. CADE desestimó el recurso dado que la operación no generaba ni reforzaba una posición dominante, pero además remarcó que, los acuerdos de confidencialidad entre Hub y Mercado Pago, las regulaciones del Banco Central y, en particular, la Ley General de Protección de Datos Personales (LGPD) alejaban la posibilidad de un uso ilícito de los datos por parte de las fusionadas. Algo similar se observa en la operación Stone-Linx, también notificada en CADE, en la que operadores competidores sostuvieron que la operación confería una ventaja competitiva a la fusionada por el acceso a datos que la misma confería. CADE descartó preocupaciones argumentando que los datos en cuestión ya se compartían en la industria de conformidad con la política de *open banking* de Brasil, y que consistentemente el dueño de los datos es el consumidor, donde la LGPD reforzará la tutela de esos datos.[19]

3.4 Relevancia de los costos anticompetitivos de la regulación para la región

El enfoque de Gal & Aviv (2020) referido a los costos competitivos de regulaciones como el RGPD obliga a plantear la discusión para la región. En este sentido, es de relevancia identificar herramientas que contribuyan a proteger la privacidad en el uso de los datos pero que al mismo tiempo no generen costos perniciosos en una región necesitada de inversión e innovación. La imposición de normativas con altos cargos para su cumplimiento podría generar altas barreras de entrada a start-ups locales, frente a BigTech globales con capacidad para ya tener implementada la GDPR. En las siguientes secciones se muestra que algunos países de la región han recibido efectivamente mucha influencia del RGPD.

17. https://www.gov.br/cade/pt-br/assuntos/noticias/bradesco-firma-acordo-com-cade-em-investigacao-de-pratica-anticompetitiva-contra-guiabolso.

18. Ato de Concentração 08700.000059/2021-55 (Magalu Pagamentos/Hub) de CADE.

19. Véase Ato de Concentração nº 08700.003969/2020-17

En ese sentido, una región necesitada de inversión e innovación debería evaluar los riesgos de implementar regulaciones potencialmente costosas.

3.5 Hechos relevantes sobre la interacción competencia-protección de datos en la región: resumen

Los países de la región muestran aún escasa evidencia de interacción entre los ámbitos de la política de competencia y de protección de datos:

	Legislaciones independientes	Privacidad como medida afectada por competencia	Legislaciones en tensión
Argentina		Medida cautelar e investigación contra Facebook- Whatsapp	
Brasil	Claro-Serasa	Recomendación conjunta de las agencias de competencia y la de protección de datos para Facebook-Whatsapp Caso Bradesco-Guiabolsa en Cade	
Chile		Fusión Uber/Cornershop	
Colombia			Recomendaciones pro-competitivas de la SIC en diversos mercados y regulaciones
El Salvador			Opinión de la SC sobre proyecto de ley de protección de datos

Tabla 2. Hechos relevantes sobre la interacción competencia-protección de datos en políticas públicas
Fuente: elaboración propia

Algunas cuestiones se deducen y destacan de la Tabla 2. Brasil es el país para el que se ha identificado una mayor cantidad de eventos de interacción. En contraste, para México y Perú no se han identificado hechos concretos de interacción.

Solo en Brasil se observa el accionar conjunto entre agencias de competencia y de protección de datos. Acciones independientes podrían llevar a pensar en consistencia con un enfoque de legislaciones independientes, mientras que la colaboración o acciones conjuntas entre agencias daría cuenta de la necesidad de coordinar esfuerzos para afrontar potenciales conflictos, como los que se deducen del enfoque de legislaciones en tensión. CADE ha presentado recientemente, un documento que plantea una comparativa internacional sobre la estructura, funciones e interrelaciones de las agencias de Defensa de la Competencia y Protección de Datos de un grupo de países (CADE, Agosto 2021), lo que evidencia la importancia que CADE le está otorgando al tema.

En el caso de Argentina, la medida preventiva de la agencia de competencia fue comunicada a la Dirección Nacional de Protección de Datos Personales. Por su parte, en Brasil la recomendación fue emitida de manera conjunta por la agencia de competencia (CADE), el Ministerio Público Fiscal (MPF), la Autoridade Nacional de Proteção de Dados (ANPD)[20],

20. Creada en 2018 por la Lei Geral de Proteção de Dados (LGPD) y con estructura aprobada en agosto 2020 por el Decreto n. 10.474, la ANPD está integrada a la Presidencia de la República y está dotada de autonomía y técnica decisoria.

y la Secretaria Nacional do Consumidor (Senacon). Esto es consistente con la tendencia más reciente que muestra acciones colaborativas entre las agencias de protección de datos y de competencia. Al respecto, en mayo de 2021, la Autoridad de Competencia y Mercados (CMA) y la Oficina del Comisionado de Información (ICO) del Reino Unido, emitieron una declaración conjunta para explicar cómo trabajarán juntos para mejorar las sinergias entre ambas agendas políticas y abordar el potencial de tensiones (CMA-ICO, 2021). En la declaración se comprometen a fomentar la cooperación y la colaboración entre las dos organizaciones y establecen un Memorando de Entendimiento. En Chile no hay una autoridad especialmente encargada de la fiscalización de la Ley de Protección de Datos aunque hay un proyecto en el Congreso para su modificación que contempla su creación. En la fusión Uber-Cornershop fue el Servicio Nacional de Consumidor (SERNAC) quien presentara antecedentes.[21] En este sentido, la herramienta del control preventivo de fusiones da cuenta de que el enforcement de las agencias de competencia aparece con más potencial preventivo que el de las agencias de privacidad.

En México, existe un potencial desafío adicional en relación con la interacción de las agencias, y es el hecho de que para los sectores de telecomunicaciones y radiodifusión la política de competencia recae en el regulador sectorial, el Instituto Federal de Telecomunicaciones (IFT) que se disputa con COFECE la competencia sobre los casos concernientes a la economía digital.[22]

Las diferentes estructuras institucionales que se observan en los países de la región, donde algunos cuentan con agencia de protección de datos y otros no, conllevan diversas implicaciones. Facuse (2020) sostiene que en Chile, dada la ausencia de una agencia de protección de datos, si la agencia de competencia no analiza los casos teniendo en cuenta la perspectiva de la protección de datos, los casos pasan sin que se haga un análisis al respecto. Por su parte, Noguera (2020) argumenta que la estructura de la SIC en Colombia con el doble rol, protección de la competencia y de la privacidad, que podía lucir en algún momento compleja, es una ventaja que permite afrontar complementariamente los desafíos que deben resolver los reguladores.

En el caso de El Salvador, al adoptar un régimen sectorizado en materia de privacidad y protección de datos personales, las funciones de supervisión y control del cumplimiento de la normatividad se encuentran distribuidas entre distintas autoridades. Este es el caso del Instituto de Acceso a la Información Pública (IAIP) por lo que se refiere al tratamiento de datos personales por parte del sector público y de quienes administran recursos públicos y ejercen actos propios de la administración pública, y la Superintendencia del Sistema Financiero respecto de los datos personales que comprenden el historial crediticio de las personas.

21. Indicó al respecto: *Finalmente, una situación altamente posible en casos de concentración es el exhaustivo intercambio de datos entre empresas, ante lo cual se requiere resguardar que los datos personales de los consumidores e información financiera sensible, sean debida y oportunamente informado a los consumidores, y su tratamiento cuente con el expreso consentimiento de los titulares* (Informe de Aprobación Uber-Cornershop de la FNE).

22. Véase Competencia Jurisdiccional de las Plataformas Tecnológicas: el caso de Uber-Cornershop, https://www.cofece.mx/wp-content/uploads/2020/07/art-Cornershop-24julio2020.pdf.

4. Legislación de protección de datos en América Latina en perspectiva con estándares internacionales

Los distintos estándares nacionales e internacionales en materia de protección de datos personales adquieren relevancia cuando la privacidad se adopta como medida afectada por la competencia, o bien, cuando la legislación de privacidad y protección de datos eleva los costos de entrada de potenciales competidores en el mercado. Mientras más elevado sea el estándar adoptado, mayores son los supuestos que podrían llegar a configurar un incumplimiento normativo que se traduzca en una afectación a la calidad de los servicios de los consumidores o usuarios. Además, la elevación de estos estándares también supone mayores costos para los agentes económicos que tratan datos personales, medidos a partir de sus obligaciones para salvaguardar el derecho a la protección de datos personales.

En la última década ha existido una tendencia creciente, tanto en el ámbito nacional como internacional, de elevar los estándares de protección de datos personales. El avance tecnológico y los riesgos que ello supone para la privacidad, han propiciado un proceso de modernización de los instrumentos internacionales pioneros en la materia, así como la emisión de nuevas legislaciones que sustituyen a las ya existentes o que incorporan, por primera vez, un régimen de protección de datos personales en su derecho interno. En ese sentido, se habla de un interés renovado en la protección de datos personales que ha abierto las puertas a una nueva generación de instrumentos normativos más acordes con la era digital (Mantelero, 2021).

En el ámbito internacional, este proceso de modernización del derecho a la protección de datos personales se evidencia a partir de la emisión y revisión de los siguientes instrumentos normativos:

a. Directrices sobre privacidad y flujos transfronterizos de datos personales, emitidas por la OCDE en 1981 y revisadas en 2013.

b. Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico (APEC), emitido en 2005 y actualizado en 2016.

c. Estándares Iberoamericanos de Protección de Datos, emitidos por la Red Iberoamericana de Protección de Datos (RIPD) en 2017.

d. Convenio No. 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981, y su Protocolo Adicional de 2001, ahora modernizados por el llamado Convenio 108+, adoptado por el Comité de Ministros el 18 de mayo de 2018.

e. Principios actualizados sobre la privacidad y la protección de datos personales, emitidos por el Comité Jurídico Interamericano (CJI) de la OEA en 2020, cuyo antecedente inmediato fueron los principios emitidos en 2012.

A todo este proceso de actualización de los instrumentos internacionales, cabe agregar la emisión y posterior entrada en vigor del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). De hecho, tanto la emisión de los Estándares Iberoamericanos de la RIPD (Martínez, 2020), como la modernización del Convenio 108 del Consejo de Europa (Consejo de Europa, *Explanatory Repor*t, 2018), tomaron como referencia este Reglamento.

Asimismo, desde la entrada en vigor del Reglamento general de protección de datos (RGPD), el 25 de mayo de 2018, varios países alrededor del mundo, entre los que se encuentran algunos de América Latina y el Caribe, se han dado a la tarea de armonizar su régimen interior conforme a este ordenamiento. Este es el caso de Brasil [Ley No. 13.709 de 14 de agosto de 2018], Uruguay [Ley No. 19.670 de 15 de octubre de 2018, que modifica la Ley No. 18.331 sobre protección de datos personales y la acción de Habeas Data], Panamá [Ley No. 81 sobre protección de datos personales, de 29 de marzo de 2019] y México por lo que se refiere específicamente al sector público [Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de 26 de enero de 2017]. Por su parte, Perú, mediante la publicación del Decreto Legislativo No. 1353 del 7 de enero de 2017, "[...] fortaleció el régimen de protección de datos personales existente hasta entonces" (Olivos, 2020). En el caso de Argentina, Chile, Colombia, El Salvador y México en el ámbito del sector privado, el tema de la protección de datos personales logró insertarse en la agenda legislativa. Sin embargo, el impulso que han recibido estas iniciativas ha estado sujeto a factores políticos que, en algunos casos, han impedido su continuidad en el debate legislativo (v.gr. el proyecto de ley de protección de datos en Argentina perdió estado parlamentario en 2020, según el estudio elaborado por el CELE en febrero de 2021).

En este contexto, si bien es innegable que el RGPD de la Unión Europea ha sido un importante referente para adoptar o, en su caso, modernizar la normatividad de la protección de datos personales en el mundo, lo cierto es que los estándares adoptados tanto en el ámbito internacional como nacional difieren entre sí.

A continuación planteamos el escenario internacional de estándares, bajo criterios comparativos que nos permitan distinguir entre distintos niveles de protección de datos personales, bajo el presupuesto de que el RGPD supone el nivel más elevado de rigidez.[23]

4.1 Estándares internacionales

Dentro de los instrumentos internacionales en materia de datos personales existen distintos niveles de desarrollo y exigencia de las responsabilidades de quienes realizan tratamientos de datos personales. Para estar en posibilidad de establecer comparativamente esos distintos niveles, tomamos como punto de referencia el RGPD a partir de los principios, categorías especiales de datos, derechos y obligaciones relativos al tratamiento de los datos personales que establece. Si bien muchas de sus disposiciones no son traspolables a los instrumentos internacionales, cuyos objetivos consisten en establecer pautas generales que guíen el diseño normativo e institucional de la legislación doméstica, estos parámetros

23. Esto es lo que Mantelero (2021), en referencia al RGPD denomina el "gold standard for data protection", dado su carácter detallado y la inclusión de normas que directamente regulan la gestión y el procesamiento de los datos personales.

dan cuenta de su estándar elevado de exigencia para salvaguardar el derecho a la protección de datos personales.

A continuación, veamos en líneas generales el contenido del RGPD en cada uno de los parámetros o rubros antes indicados, a fin de contrastar dicho contenido con respecto a las disposiciones contenidas en los instrumentos internacionales que presentan mayor relevancia para los países de la región sujetos a este análisis.

Cabe señalar que los instrumentos internacionales que hemos seleccionado son: el Convenio 108 en su versión actualizada (Convenio 108+), las Directrices de la OCDE en materia de protección de datos personales, los Estándares Iberoamericanos de Protección de Datos de la RIPD, así como los Principios Actualizados de la OEA, dada su relevancia en el impulso y visión para la generación de estándares comunes en materia de protección de datos personales en LATAM.

4.1.1 Principios del derecho a la protección de datos

El artículo 5 del RGPD establece los principios que rigen el tratamiento de los datos personales. De manera desagregada, estos principios son los siguientes:

a. **Licitud**. Este principio parte de la idea de que el tratamiento de los datos personales sólo puede realizarse si se cuenta con el consentimiento de los titulares de los datos personales o con una base legítima que lo justifique, como podría ser la ejecución de un contrato, una disposición normativa habilitante o para la satisfacción de intereses legítimos (Artículo 6 del RGPD). Cabe advertir que el RGPD no admite la figura del consentimiento tácito o implícito. En cualquier caso, éste debe de ser expreso.

b. **Lealtad**. Este principio exige que el tratamiento de los datos personales por parte del responsable se realice de manera leal, sin acudir a medios fraudulentos o desleales.

c. **Transparencia**. Este es uno de los principios que mayor relevancia ha adquirido ante el avance tecnológico y las novedades que trajo consigo el RGPD. Si bien pone énfasis en la información que los responsables deben proporcionar a los titulares de datos personales respecto de su identidad, las finalidades del tratamiento y los mecanismos para hacer valer los derechos de los interesados, también implica que los titulares "deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento" (Considerando 39 del RGPD).

d. **Limitación de la finalidad**. En términos generales, las finalidades del tratamiento de los datos personales deben de ser explícitas y legítimas. Por supuesto, estas finalidades también deben de ser transmitidas con claridad a los titulares de los datos, en concordancia con el principio de transparencia.

e. **Minimización de los datos**. El responsable del tratamiento sólo puede tratar aquellos datos personales que resulten adecuados, pertinentes y limitados a los fines previamente determinados o que resulten compatibles con estos fines. Este principio es equivalente al también denominado principio de proporcionalidad en otros ordenamientos jurídicos.

f. **Exactitud**. Este principio implica el deber de los responsables del tratamiento de mantener los datos exactos y actualizados. Suele ser equivalente, al menos en parte de su contenido, respecto del llamado principio de calidad en otros ordenamientos jurídicos.

g. **Limitación del plazo de conservación**. Este principio supone que los responsables de los datos personales deben establecer plazos específicos en los que podrán conservar los datos personales, en concordancia con las finalidades para los cuales fueron recabados. La implementación de este principio resulta altamente compleja para aquellas organizaciones que cuentan con diversas bases de datos e información de muy distinta naturaleza.

h. **Integridad y confidencialidad**. Este principio exige la implementación de medidas de seguridad adecuadas para salvaguardar la integridad, disponibilidad y confidencialidad de la información personal. Para determinar si las medidas adoptadas han sido efectivamente adecuadas, es necesario que el responsable del tratamiento tome en consideración, entre otros factores, el riesgo o la gravedad de una posible incidencia de seguridad (Artículo 32 del RGPD).

i. **Responsabilidad proactiva**. A partir de este principio se derivan una serie de obligaciones para los responsables del tratamiento de datos personales que implican la adopción de medidas técnicas y organizativas que les permitan, además de cumplir con las disposiciones del Reglamento, demostrar dicho cumplimiento. Entre otras, este principio supone el registro de actividades del tratamiento que permitan su seguimiento y, en su caso, supervisión.

Al tratarse de los pilares de construcción del derecho a la protección de datos personales y tener una interpretación abierta, existe una tendencia general en adoptar estándares homogéneos respecto de los principios que rigen este derecho. Si bien existen diferencias en cuanto a su categorización y alcance respecto de las obligaciones que se establecen a partir de ellos, los instrumentos internacionales en materia de protección de datos personales, que mayor influencia reciente han tenido o pretenden tener en el proceso de modernización o incorporación legislativa de los países de Latinoamérica, comprenden estos principios en sus textos.

RGPD (Unión Europea)	Convenio 108+ (Consejo de Europa)	Directrices (OCDE)	EIPD (RIPD)	Principios actualizados (OEA)
Licitud	✓	✓	✓	✓
Lealtad	✓	✓	✓	✓
Transparencia	✓	✓	✓	✓
Limitación de la finalidad	✓	✓	✓	✓
Minimización de los datos	✓	✓	✓	✓
Exactitud	✓	✓	✓	✓
Limitación del plazo de conservación	✓	✗	✓	✓
Integridad y confidencialidad	✓	✓	✓	✓
Responsabilidad	✓	✓	✓	✓

Tabla 3. Principios del derecho a la protección de datos en los estándares internacionales.
Fuente: elaboración propia

No obstante, en las Directrices de la OCDE se advierte la ausencia del principio de limitación del plazo de conservación. La previsión de plazos fue objeto de un amplio debate entre los integrantes del grupo revisor de las Directrices. Además, se consideró como un aspecto que podía constituir un nivel distinto al que corresponde a los principios básicos del derecho a la protección de datos personales, por lo que su incorporación podía quedar sujeta a la legislación doméstica de los Estados parte (OECD, 2013).

4.1.2 Categorías especiales de datos

El artículo 9 del RGPD establece, como regla general, la prohibición de usar, almacenar y procesar información de las categorías especiales de datos (también llamados datos sensibles). Estas categorías comprenden aquellos datos que "revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física".

Esta misma disposición establece taxativamente las excepciones a la prohibición general del tratamiento de datos personales sensibles e incorpora algunas condiciones específicas para poder tratarlos que constituyen un régimen reforzado que, a su vez, supone la adopción de mayores medidas de protección para los responsables del tratamiento.

De igual forma, en su artículo 10, el RGPD introduce un régimen reforzado para el tratamiento de datos personales relativos a condenas e infracciones en el ámbito penal. Este régimen sujeta el tratamiento de este tipo de información a la supervisión de las autoridades públicas, o bien, que cuenten con un fundamento normativo en el que se hayan adoptado garantías adecuadas para los derechos y libertades de los interesados.

En términos generales, la adopción de categorías especiales de datos se encuentra en el modelo europeo desde los instrumentos pioneros en la materia, con excepción de los datos personales relativos a condenas e infracciones en el ámbito penal cuya atención es relativamente reciente. Este es el caso del Convenio 108 del Consejo de Europa en su versión original, así como de la antecesora del RGPD, la Directiva 95/46 CE, que ya establecían un régimen reforzado para ciertas categorías de datos. No obstante, su inclusión, alcance y las condiciones del tratamiento de este tipo de información en los instrumentos internacionales ha sido objeto de debate. No todos estos instrumentos participan de la idea de reconocer categorías específicas de datos personales sujetos a un régimen reforzado, pues consideran que su desarrollo debe abordarse fundamentalmente a partir de la legislación doméstica.

En la siguiente tabla podemos observar de manera resumida cómo se ha abordado el tema en los distintos instrumentos internacionales seleccionados.

RGPD (Unión Europea)	Convenio 108+ (Consejo de Europa)	Directrices (OCDE)	EIPD (RIPD)	Principios actualizados (OEA)
Alcance de la definición (Limitativa)	Enunciativa	No incluye esta categoría	Enunciativa	Enunciativa (sin mención a ciertos tipos de datos)
Prohibición de tratamiento como regla general y excepciones	No establece la prohibición como regla general	No establece la prohibición como regla general	Sí comprende la prohibición como regla general y sus excepciones	No establece la prohibición como regla general
Condiciones específicas para el tratamiento (Régimen reforzado)	Régimen reforzado	No establece un régimen reforzado	Régimen reforzado	Régimen reforzado (sin establecer condiciones específicas)

Tabla 4: categorías especiales de datos en los estándares internacionales
Fuente: elaboración propia

De conformidad con la Tabla 4, las Directrices de la OCDE no incluyen una definición equiparable a las categorías especiales de datos. El Grupo de Expertos que llevó a cabo la revisión de 2013 de este instrumento consideró que no era factible identificar categorías que universalmente pudieran considerarse sensibles (OECD, 2013). En consecuencia, estas Directrices no incorporan ningún régimen específico para este tipo de información, a pesar de que reconocen la necesidad de que el tratamiento de datos personales esté sujeto a límites.

En el caso de los Principios Actualizados de la OEA, el Principio Nueve hace referencia a los datos personales sensibles. Si bien reconoce la necesidad de establecer un régimen reforzado para este tipo de información en la legislación doméstica de los Estados parte, lo cierto es que no establece criterios que permitan identificar qué datos personales deben de ser considerados bajo esta categoría, ni las condiciones específicas para su tratamiento. Así, este instrumento encomienda su desarrollo normativo a los Estados parte.

4.1.3 Obligaciones de los responsables del tratamiento

El RGPD establece diversas obligaciones para los responsables del tratamiento de datos personales, sea a partir del desarrollo de los principios, o bien, como una forma específica de salvaguardar el debido uso, procesamiento o almacenamiento de la información. Se desglosan a continuación algunas de las obligaciones previstas por el RGPD que por su novedad, elevado costo y complejidad de implementación, ameritan una mención especial.

a. **Protección de datos desde el diseño y por defecto**. Esta obligación supone la adopción de medidas técnicas y organizativas que permitan salvaguardar la privacidad al desarrollar, diseñar e implementar aplicaciones, productos o servicios que traten de datos personales (Considerando 78 del RGPD). Se trata de incorporar la privacidad como un objetivo a seguir dentro de cualquier sistema tecnológico o práctica comercial. Su cumplimiento se relaciona con el principio de responsabilidad proactiva, pues permite a los desarrolladores cumplir con las demás disposiciones del RGPD. Estas medidas deben de adoptarse teniendo en cuenta "el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa

probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas." (Artículo 25 del RGPD).

b. **Evaluación de impacto relativa a la protección de datos personales**. Esta obligación está dirigida a los responsables que realizan tratamientos de datos personales que entrañan un alto riesgo para los derechos y libertades de las personas físicas, como puede ser el procesamiento o almacenamiento, a través de nuevas tecnologías, de datos personales sensibles, o que evalúan de manera sistemática o exhaustiva aspectos personales de los consumidores o usuarios, o para el control de zonas de acceso público a gran escala. Su cumplimiento consiste en evaluar el riesgo del tratamiento y su posible impacto, así como la necesidad y proporcionalidad del tratamiento con respecto a su finalidad. Si el resultado de la evaluación determina que el tratamiento constituye un elevado riesgo, el responsable debe consultar a la autoridad de control antes de efectuar el mismo (obligación de consulta previa). Asimismo, las medidas técnicas y organizativas adoptadas por el responsable deben adecuarse a estos resultados. (Considerandos 84 y 91 del RGPD y Artículo 35 del RGPD).

c. **Seguridad del tratamiento**. Los responsables y encargados del tratamiento de datos personales deben adoptar medidas técnicas y organizativas apropiadas para salvaguardar la integridad, confidencialidad, disponibilidad y resiliencia de los sistemas y servicios del tratamiento. Estas medidas deben de ser acordes con la probabilidad y gravedad del riesgo que supone el tratamiento. Asimismo, deben de tomar en consideración el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento. Adicionalmente, la seguridad del tratamiento conlleva la obligación de verificar, dar seguimiento y, en su caso, actualizar las medidas técnicas y organizativas, de manera periódica. (Artículo 32 del RGPD).

d. **Notificación de violaciones a la seguridad de los datos**. El RGPD establece la obligación de notificar a las autoridades de control de todas aquellas vulneraciones a la seguridad de los datos personales en aquellos casos en los que dicha vulneración entrañe un riesgo para los derechos y libertades de las personas físicas. Si el riesgo es alto, esta vulneración también deberá de ser notificada a los titulares de los datos personales. Asimismo, sin importar el nivel de riesgo, toda vulneración debe de ser documentada a partir de los hechos y sus efectos, así como las medidas correctivas adoptadas. (Artículo 33 del RGPD)

e. **Designación de delegado de protección de datos personales**. El RGPD establece las condiciones a partir de las cuales los responsables y encargados del tratamiento de datos personales deben designar un oficial de protección de datos personales. En general, deben cumplir con esta obligación los órganos, organismos e instituciones públicas, con excepción de los tribunales por lo que hace a su función jurisdiccional; quienes realicen tratamientos a gran escala de categorías especiales de datos personales, y todos aquellos cuyo tratamiento, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de titulares de datos a gran escala (Artículo 35 del RGPD). Las funciones del delegado de protección de datos son, en términos generales, de supervisión y asesoramiento del responsable y el encargado para el cumplimiento de los principios y obligaciones del derecho a la protección de datos, así como de cooperación con las autoridades de control (Artículo 39 del RGPD).

El principio de responsabilidad proactiva y la incorporación de medidas de seguridad técnicas son algunos de los aspectos que han guiado la actualización de los estándares que rigen el derecho a la protección de datos personales de conformidad con el avance de las tecnologías de la información y comunicación. Ello explica por qué la mayoría de los

instrumentos internacionales modernizados incorporan en sus textos obligaciones relativas a los sistemas de seguridad informática, a la prevención de pérdidas, daños y accesos no autorizados, así como a la adopción de medidas técnicas y organizativas que incorporen objetivos de privacidad en su diseño y por defecto (Tabla 5).

De hecho, la actualización de las Directrices de la OCDE en 2013 pone énfasis en la introducción de un *privacy management programme*, sujeto a revisión periódica, que incluya la adopción de salvaguardas apropiadas conforme a un *privacy risk assessment* y las medidas que interioricen preocupaciones sobre privacidad en los nuevos desarrollos que supongan el tratamiento de datos personales. De igual forma, los Estándares Iberoamericanos de Protección de Datos reconocen específicamente "la importancia de la adopción de medidas preventivas que permitan al responsable responder proactivamente ante los posibles problemas relacionados con el derecho a la protección de datos personales como son [...] la designación de un oficial de protección de datos personales y la privacidad por defecto y por diseño, entre otras, lo cual resulta esencial en el ámbito de las tecnologías de la información y las telecomunicaciones" (Considerando 23 de los EIPD). En el caso de los principios actualizados de la OEA, dada la naturaleza de su contenido, no desarrolla los deberes y obligaciones que surgen a partir del principio de responsabilidad. Sin embargo, en cuanto a la seguridad de los datos, establece a grandes rasgos que los Estados parte deben adoptar "salvaguardias de seguridad técnicas, administrativas, u organizacionales razonables y adecuadas", las cuales deberían de ser objeto de auditorías y actualización permanente (Principio Seis).

RGPD (Unión Europea)	Convenio 108+ (Consejo de Europa)	Directrices (OCDE)	EIPD (RIPD)	Principios actualizados (OEA)
Protección de datos desde el diseño y por defecto	✓	✓	✓	✗
Evaluación de impacto relativa a la protección de datos personales	✓	✓	✓	✗
Seguridad del tratamiento	✓	✓	✓	✓
Notificación de violaciones a la seguridad de los datos (Autoridad de control y titulares de datos)	✓ (Autoridad de control)	✓ (Autoridad de control y titulares de datos)	✓ (Autoridad de control y titulares de datos)	✗
Designación de delegado de protección de datos personales	✗	✗	✓	✗

Tabla 5: obligaciones de los responsables del tratamiento en los estándares internacionales
Fuente: elaboración propia

Cabe enfatizar que a pesar de que los instrumentos internacionales seleccionados prevén un gran número de las obligaciones previamente indicadas, las condiciones para su exigibilidad, así como los mecanismos para darles cumplimiento quedan al arbitrio de las legislaciones internas de los Estados parte. No obstante, los EIPD se aproximan de manera más evidente a los estándares fijados por el RGPD, dado que establecen con un mayor desarrollo algunas de estas obligaciones, como es el caso de la designación del delegado de protección de datos, sobre el cual introduce sus funciones, así como por lo que se refiere a las notificaciones de vulneraciones a la seguridad.

4.1.4 Distinción en los niveles de estándares internacionales

A partir de las diferencias y coincidencias entre los distintos instrumentos internacionales seleccionados, con respecto al RGPD, podemos advertir distintos niveles en los estándares que guían el desarrollo normativo del derecho a la protección de datos personales, donde los EIPD son los que mayor cercanía presentan con respecto al RGPD (Nivel 1), seguido por el Convenio 108+ (Nivel 2), posteriormente las Directrices de la OCDE (Nivel 3) y, finalmente, los Principios actualizados de la OEA (Nivel 4). Sin embargo, no debe pasar desapercibido que mientras el Convenio 108+ tiene un carácter vinculante para sus Estados parte, los demás instrumentos constituyen normas de *soft law*.

La Tabla 6 reporta el grado de proximidad de cada uno de los instrumentos internacionales al RGPD, a partir de asignar el valor de 1 punto a cada coincidencia o 0.5 para las parcialmente cercanas.

	Convenio 108+ (Consejo de Europa)	Directrices (OCDE)	EIPD (RIPD)	Principios actualizados (OEA)
Principios	9	8	9	9
Categorías especiales de datos	1.5	0	2.5	1
Obligaciones	3.5	4	5	1
Total	14	12	16.5	11

Tabla 6: Niveles de estándares internacionales relativos al RGPD
Fuente: elaboración propia.

De acuerdo con la información de la Tabla 6, los Estándares Iberoamericanos de Protección de Datos, elaborados en el seno de la Red Iberoamericana de Protección de Datos, son los que presentan una mayor coincidencia con el RGPD. En segundo lugar, el Convenio 108 modernizado adopta muchos de los estándares de este ordenamiento, pero sin perder con ello su vocación universal que admite la incorporación de terceros países, no miembros del Consejo de Europa , aunque con elementos cercanos al modelo europeo. Tanto las Directrices de la OCDE y los Principios del Comité Jurídico Interamericano de la OEA establecen estándares menores de protección, procurando centrarse en pisos mínimos realizables por sus Estados parte, aún cuando sus sistemas jurídicos se distancian del modelo regulatorio centralizado de Europa.

4.2 Adecuación de la legislación doméstica con los estándares internacionales

A continuación se detalla en dónde se ubican las respectivas legislaciones del grupo de países considerados, de conformidad con los parámetros establecidos en los incisos anteriores.

4.2.1 Argentina

Argentina fue el primer país en obtener el reconocimiento de un nivel adecuado de protección para la realización de transferencias internacionales con Europa. De manera reciente, mediante ratificación del 25 de febrero de 2019, se adhirió al Convenio 108 del Consejo de Europa en sus términos originales. Asimismo, cabe señalar que es miembro activo tanto de la OEA como de la Red Iberoamericana de Protección de Datos (RIPD).

Dentro de la normatividad que rige el derecho a la protección de datos personales destaca la siguiente[24]:

a. Ley 25.326, del 2 de noviembre de 2000, de Protección de Datos – modificada por la Ley 26.343, de 8 de enero de 2008.

b. Decreto 1558/2001, de 29 de noviembre de 2001, Reglamentación de la Ley de protección de datos.

c. Decreto No. 746, del 25 de septiembre de 2017, de atribución a la Agencia de Acceso a la Información Pública (AAIP), de las competencias de control y supervisión en materia de protección de datos personales.

Dada su pertenencia al Convenio 108 del CE, Argentina ha adaptado su legislación interna a los estándares europeos. Este modelo ha sido un importante referente en la forma en la que aborda normativamente el derecho a la protección de datos personales. Ello se observa en la adopción de la totalidad de los principios previamente identificados, incluyendo la especificación de un plazo para la conservación de los datos personales y el consentimiento expreso. Aunque el principio de minimización de los datos personales está referido específicamente a los datos personales sensibles.

Asimismo, adopta una definición limitativa de datos sensibles, aunque no incorpora algunas categorías contempladas actualmente por el RGPD, como es el caso de los datos genéticos. Finalmente, por lo que hace a las obligaciones de los responsables del tratamiento de datos personales, la legislación en materia de datos personales sólo hace referencia a la necesidad de adoptar medidas de seguridad para salvaguardar la confidencialidad, integridad y disponibilidad de la información personal, pero no incorpora la obligación de notificación de vulneraciones a la seguridad. Tampoco se encuentran de manera explícita en su texto normativo las obligaciones derivadas del principio de responsabilidad proactiva, tales como la elaboración de evaluaciones de impacto a la protección de datos o la adopción de medidas de privacidad desde el diseño y por defecto.

En conclusión, si bien Argentina ha tenido una fuerte influencia a partir del modelo europeo de protección de datos personales en sus términos originales, su régimen normativo vigente aún no adapta sus disposiciones de conformidad con los instrumentos internacionales actualizados, específicamente por lo que hace a las obligaciones de los responsables del tratamiento de datos personales.

24. La legislación de Argentina en materia de protección de datos personales puede consultarse en: https://www.redipd.org/es/legislacion.

4.2.2 Brasil

Brasil es uno de los países seleccionados que cuenta con una reciente adopción del régimen de protección de datos personales en su legislación interna. Su legislación en la materia, además de algunas disposiciones de carácter sectorial previamente existentes, es la siguiente:

a. Ley General de Protección de Datos Personales No. 13.709, de 14 de agosto de 2018, que modifica la Ley nº 12.965, de 23 de abril de 2014 (Marco Civil de Internet).

b. Medida provisoria No. 869, de 27 de diciembre de 2018, por la que se crea la Autoridad Nacional de Protección de Datos y se prorroga a los dos años la entrada en vigor de la Ley No. 13.709.

A pesar de no ser parte del Convenio 108 del Consejo de Europa, su reciente legislación toma como referentes tanto al RGPD como al Convenio 108 en su versión modernizada. En términos generales, incluye todos los principios del derecho a la protección de datos personales, con excepción de la obligación de establecer un periodo de conservación de los datos. No obstante, este último se introduce como una hipótesis a partir de la cual concluye el tratamiento de los datos personales. En cuanto al consentimiento, la Ley No. 13.709 sólo establece el consentimiento expreso y por escrito para algunos supuestos específicos, lo cual implica el reconocimiento del consentimiento tácito en los demás casos.

Asimismo, la legislación brasileña introduce una definición limitativa de los datos personales sensibles, en la cual incorpora categorías propias del RGPD tales como los datos genéticos y biométricos. A esto añade un régimen reforzado a partir de los principios y obligaciones de los responsables del tratamiento de los datos personales.

Finalmente, por lo que hace a las obligaciones de los responsables y encargados del tratamiento, la Ley No. 13.709 recoge las obligaciones previstas por el RGPD, antes abordadas, entre las que se incluyen la realización de evaluaciones de impacto a la protección de datos personales, la adopción de medidas de seguridad, la notificación de incidentes tanto a la autoridad de control como a los titulares de los datos personales, así como el nombramiento de un oficial de protección de datos. Si bien no contempla de manera explícita la privacidad desde el diseño y por defecto, esta ley habilita a los responsables y encargados del tratamiento (denominados controlador y procesador, respectivamente) para adoptar programas de gobernanza en privacidad que fortalezcan el principio de responsabilidad proactiva.

En conclusión, Brasil adopta un régimen de protección de datos personales cercano a las preocupaciones manifestadas en los procesos de modernización de los instrumentos internacionales seleccionados. Además, se advierte un cercano impacto del modelo europeo en su diseño normativo. No obstante, la legislación brasileña adopta ciertas particularidades que flexibilizan el régimen adoptado por el RGPD, pues, entre otras cosas, exceptúa de su régimen de aplicación el tratamiento de datos para fines académicos, periodísticos o artísticos. En otras palabras, esta legislación no puede ser considerada como una copia del RGPD.

4.2.3 Chile

La legislación especial en materia de datos personales de Chile, además de otras disposiciones de carácter sectorial, se encuentra en la Ley No. 19.628, publicada el 28 de agosto de 1999, sobre protección de la vida privada. Si bien esta ley ha sido reformada en múltiples ocasiones[25], lo ha hecho en aspectos muy específicos que impactan de manera limitada el régimen general de la protección de datos personales, con excepción de la Ley 20.575 que establece el principio de finalidad en el tratamiento de datos personales, publicada el 17 de febrero de 2012.

Por lo que se refiere a los principios que guían el derecho a la protección de datos personales, la Ley No. 19.628 no establece el principio del plazo de conservación ni el principio de responsabilidad en su carácter proactivo o demostrable. En cuanto al principio de integridad y confidencialidad, este ordenamiento "sólo contempla [...] una obligación general de seguridad de datos personales que le imponen al responsable del banco de datos: i) cuidar de ellos con la debida diligencia; y ii) hacerse responsable de los daños" (Benussi, 2020). Además, por lo que hace al consentimiento para el tratamiento de los datos personales establece, como regla general, que la autorización sea por escrito.

En cuanto al régimen de categorías especiales de datos, la legislación chilena adopta una definición de datos sensibles en la cual incorpora de manera diferenciada a otras disposiciones de derecho comparado, las circunstancias que atañen a la vida privada o la intimidad de las personas, tales como los hábitos personales (Artículo 2, inciso g). Se trata así, de una categoría abierta susceptible a interpretación. Finalmente, por lo que se refiere a las obligaciones de los responsables del tratamiento de datos personales no se advierten de manera explícita ninguna de las previamente seleccionadas conforme al RGPD en las disposiciones de la Ley No. 19.628. No obstante, las obligaciones de seguridad se encuentran dispersas en algunas leyes de carácter sectorial[26], o bien, se desprenden, fundamentalmente, de las obligaciones de reserva o confidencialidad de los datos objeto del tratamiento (Benussi, 2020).

En conclusión, el régimen normativo de Chile difiere sustantivamente del RGPD, así como de las novedades introducidas por el Protocolo modificatorio del Convenio 108 y demás instrumentos internacionales modernizados. A pesar de contar con un régimen general en materia de protección de datos personales, gran parte de su desarrollo normativo se lleva a cabo a través de leyes sectoriales.

25. Véase la Ley No. 19.812, publicada el 13 de junio de 2002, que modifica la ley N° 19.628; Ley No. 20.463, publicada el 25 de octubre de 2010, que modifica la ley Nº 19.628, suspendiendo por el plazo que indica la información comercial de las personas cesantes; Ley No. 20.521, publicada el 23 de julio de 2011, que modifica la ley Nº 19.628, para garantizar que la información entregada a través de predictores de riesgo sea exacta, actualizada y veraz; Ley No. 20.575, publicada el 17 de febrero de 2012, que establece el principio de finalidad en el tratamiento de datos personales, modificando la ley N° 19.628; Ley No. 21.214, publicada el 28 de febrero de 2020, que modifica la ley N° 19.628, con el objeto de prohibir que se informe sobre las deudas contraídas para financiar la educación en cualquiera de sus niveles; entre otras disposiciones de carácter sectorial. Estas disposiciones pueden consultarse en: https://www.redipd.org/es/legislacion?nid=78.

26. Véase la Ley 21.180 sobre Transformación Digital del Estado y el Decreto Supremo 83 de la Secretaría General de la Presidencia de 2005, a través del cual "aprueba norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.

4.2.4 Colombia

Actualmente Colombia preside la Red Iberoamericana de Protección de Datos. Su normatividad en materia de datos personales se encuentra fundamentalmente en los siguientes instrumentos[27]:

a. Ley 1581, de 17 de octubre de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.

b. Decreto 1377, de 27 de junio de 2013, por el cual se reglamenta parcialmente la Ley Nº 1581.

c. Decreto 886 del 13 de mayo de 2014, por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.

d. Decreto 090 del 18 de enero de 2018, por el cual se modifican los artículos 2.2.2.26.1.2 y 2.2.2.26.3.1 del Decreto 1074 de 2015 - Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.

La Superintendencia de Industria y Comercio ha emitido numerosas guías en aspectos específicos para el tratamiento de datos personales, como son el cómputo en la nube, comercio electrónico, tratamientos con fines de marketing y publicidad, así como para la implementación del principio de responsabilidad demostrada. En ese contexto, el régimen normativo de Colombia sigue, en términos generales, los principios de la protección de datos personales. Su legislación, a diferencia de otros ordenamientos de derecho comparado en la región, establece específicamente el término de "responsabilidad demostrada". Asimismo, comprende la minimización de datos especialmente por lo que se refiere a las categorías especiales de datos. En cuanto al consentimiento, éste debe otorgarse por signos inequívocos, sin que el silencio pueda llegar a constituirlo. Si bien ni la ley ni el reglamento establecen de manera explícita la obligación de informar al titular sobre los plazos de conservación, sujeta el tratamiento de los datos a cuando ello sea razonable y necesario de acuerdo con sus finalidades. En cuanto a las categorías especiales de datos, las disposiciones normativas de Colombia, incorporan una definición enunciativa de datos sensibles, bajo un régimen reforzado para su tratamiento.

Finalmente, por lo que hace a las obligaciones tanto la ley como su reglamento comprenden la obligación de notificar a la Superintendencia de Industria y Comercio sobre las violaciones a los códigos de seguridad cuando existan riesgos en la administración de la información. Al respecto cabe decir que el Decreto 1377 introduce una cláusula habilitante mediante la cual esta autoridad podrá emitir instrucciones relacionadas con las medidas de seguridad. Si bien no menciona de manera explícita la privacidad desde el diseño y por defecto o las evaluaciones de impacto a la privacidad, ha sido un impulsor de su adopción a partir de normas de soft law. Además, el reglamento introduce un capítulo específico para la responsabilidad demostrada, cuya implementación considera la evaluación de los riesgos potenciales y exige la adopción de políticas internas efectivas.

27. Estas disposiciones pueden consultarse en: https://www.redipd.org/es/legislacion?nid=83.

4.2.5 El Salvador

La República de El Salvador adopta un modelo regulatorio sectorial. Carece de un ordenamiento que establezca un régimen general para el tratamiento de los datos personales. Algunas disposiciones relevantes del tema pueden encontrarse en[28]:

a. Decreto No. 534, de 30 de marzo de 2011. Ley de Acceso a la Información Pública (en especial, su Título III, dedicado a la Protección de Datos Personales).

b. Decreto No. 136, de 1 de septiembre de 2012. Reglamento de la Ley de Acceso a la Información Pública.

c. Decreto Legislativo No. 695, de 27 de julio de 2011. Ley de regulación de los Servicios de Información sobre el Historial de Crédito de las Personas.

d. Decreto Legislativo No. 166, de 8 de septiembre de 2005. Ley Protección al Consumidor.

e. Decreto Legislativo No. 142, de 6 de noviembre de 1997 (reformada en 2008). Ley Telecomunicaciones y Energía.

f. Decreto Legislativo No. 1030, de 26 de abril de 1997. Código Penal. Delitos relativos a la intimidad. Ha sufrido diversas reformas parciales, la última en diciembre de 2013.

g. Reglamento General de Ley Penitenciaria. Establece algunas disposiciones sobre privacidad de datos del interno.

La Ley de Acceso a la Información Pública comprende dentro de sus objetivos la protección de los datos personales que se encuentren en posesión de los entes públicos o que administren recursos públicos o realicen actos propios de la administración pública. De esta forma, el régimen al que se sujetan los datos personales atiende fundamentalmente a la necesidad de clasificar la información como confidencial frente al ejercicio del derecho de acceso a la información pública. Así, este ordenamiento le otorga primacía al principio de máxima publicidad. Sus disposiciones carecen de un catálogo de principios. Sin embargo, establece una definición de datos personales sensibles bajo categorías abiertas que admiten su interpretación, a fin de reforzar la confidencialidad y seguridad de este tipo de información. Asimismo, la Ley de Acceso a la Información pública establece algunas obligaciones para el sector público o para quienes administren recursos públicos o ejecuten actos administrativos, tales como la exigencia de informar a las personas la finalidad del tratamiento de sus datos y la adopción de medidas de seguridad.

Las disposiciones más elaboradas en la protección de datos se encuentran en la Ley de Regulación de los Servicios de Información sobre el Historial de Crédito de las Personas. En este ordenamiento se establecen las definiciones, principios y deberes que rigen el tratamiento de la información relativa al historial de crédito de las personas. Esta ley introduce algunos de los principios previamente indicados en los instrumentos internacionales, tales como el de exactitud, finalidad, información y seguridad de los datos. No obstante, se distancia significativamente de los principios recogidos por el RGPD y los instrumentos internacionales seleccionados, pues los aborda a partir de los deberes y obligaciones de las Agencias de Información de Datos sobre Historial de

28. Estas disposiciones pueden consultarse en: https://www.redipd.org/es/legislacion?nid=79.

Crédito y los agentes económicos que traten este tipo de información. Las obligaciones están fundamentalmente dirigidas a garantizar la confidencialidad, seguridad y acceso de los titulares de la información. Si bien este ordenamiento no introduce una categoría específica de datos sensibles, considera un régimen reforzado para lo que denomina "datos negativos" del historial de crédito.

Dado este contexto, la República de El Salvador establece un régimen de protección de datos personales sectorizado con estándares por debajo del RGPD y los instrumentos internacionales seleccionados para este análisis. Así, se distancia del modelo europeo de protección de datos, cuya regulación centralizada supone como problemático cualquier tratamiento de datos personales.

4.2.6 México

En el año 2018, México se adhirió al Convenio 108 del Consejo de Europa en su versión original. Asimismo, al igual que en el caso de Colombia, es parte de la OCDE. En consecuencia, sus disposiciones normativas han tenido una fuerte influencia tanto del ámbito europeo como a partir de este organismo internacional de carácter global. Su régimen normativo respecto del derecho a la protección de datos personales está fragmentado. Por una parte, existe una legislación específica para el sector privado, con un alcance federal y, por la otra, cuenta con distintas leyes dirigidas al sector público tanto en el ámbito federal como estatal. No obstante, estas últimas se encuentran homologadas con base en una ley general que establece los principios, derechos y obligaciones de los responsables y encargados del tratamiento de los datos personales del sector público.[29]

Los ordenamientos especiales en materia de protección de datos personales para el sector privado son:

a. Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), publicada en el Diario Oficial de la Federación, el 5 de julio de 2010.

b. Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicada en Diario Oficial de la Federación, el 21 de diciembre de 2011.

El régimen normativo aplicable para el sector público se encuentra fundamentalmente en los siguientes ordenamientos:

a. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), publicada en el Diario Oficial de la Federación, el 26 de enero de 2017.

b. Lineamientos Generales de Protección de Datos Personales para el Sector Público, publicados en el Diario Oficial de la Federación, el 26 de enero de 2018.

c. Diversa legislación en materia de protección de datos personales en cada una de las 32 entidades federativas, homologada a la Ley General de 2017.

29. El régimen normativo de México en materia de protección de datos personales puede consultarse en: https://www.redipd.org/es/legislacion?nid=85.

La LGPDPPSO, dada su fecha de creación y la influencia directa del RGPD de la Unión Europea, introduce estándares más elevados que la LFPDPPP. No obstante, esta última se encuentra adecuada a lo dispuesto por el Convenio 108 del Consejo de Europa y su Protocolo, en sus términos originales.

En el caso de la LGPDPPSO existe coincidencia en cuanto a los principios incorporados en el RGPD y los instrumentos internacionales seleccionados. Este ordenamiento desarrolla de manera reforzada los principios de responsabilidad proactiva, transparencia (o información), seguridad y establece la necesidad de especificar plazos de conservación de los datos personales.

Con base en estos principios, la Ley incorpora las obligaciones que establece el RGPD, incluida la designación del oficial de protección de datos, la evaluación de impacto a la protección de datos y la privacidad desde el diseño y por defecto. Asimismo, establece las condiciones a partir de las cuales debe cumplirse con estas obligaciones, relacionadas con la naturaleza de los datos (esto es, si son sensibles) y con su tratamiento intensivo o relevante.

Por su parte, la LFPDPPP y su Reglamento comprenden los principios que guían la protección de datos personales antes indicados, aunque su desarrollo, a través de los deberes de los responsables de datos personales, encuentra algunas limitaciones. Estas disposiciones no comprenden la obligación de elaborar evaluaciones de impacto a la protección de datos personales ni la designación del oficial de protección de datos.

En ambos casos se establece un régimen reforzado para el tratamiento de datos personales sensibles, definidos de manera enunciativa en la legislación, de tal forma que ello ha permitido extender sus alcances a ciertos tipos de datos (como los datos biométricos) aún cuando no sean explícitos. Los datos sensibles requieren del consentimiento expreso del titular, por lo que constituyen una excepción a la regla general que admite el consentimiento tácito.

En conclusión, México ha tenido una fuerte influencia del modelo regulatorio europeo con el objeto de elevar los estándares de protección de la información personal, aún cuando se observan algunas diferencias, como la posibilidad de admitir el consentimiento tácito de los titulares de los datos.

4.2.7 Perú

La legislación especial en materia de datos personales de Perú, además de otras disposiciones de carácter sectorial, se encuentra en la Ley No. 29733 de Protección de Datos Personales, así como su modificación, mediante el Decreto legislativo No. 1351. También cuenta con el Reglamento de la Ley 29733, emitido mediante el Decreto Supremo No. 003-2013-JUS, de 21 de marzo de 2013.[30]

Si bien estas disposiciones incorporan un catálogo de los principios rectores de la protección de datos personales, establecen que éstos sólo tendrán un carácter enunciativo, abriendo así la puerta a un mayor desarrollo que permita su adecuación a los estándares internacionales. Asimismo, para el tratamiento de los datos personales se requiere el

30. Estas disposiciones pueden consultarse en: https://www.redipd.org/es/legislacion?nid=86.

consentimiento expreso del titular, con las excepciones establecidas en la propia ley. De igual forma, la ley en la materia establece una definición de datos sensibles limitativa, en la cual incorpora algunas de las categorías a las que se refiere el RGPD como son los datos biométricos. Para estos casos, el consentimiento debe de ser por escrito.

Esta legislación no incluye obligaciones relativas a la evaluación de impacto a la protección de datos personales, la designación del oficial de datos o la notificación de vulneraciones. Sin embargo, introduce cláusulas habilitantes por las cuales permite que sea la Autoridad Nacional de Protección de Datos, quien establezca los requisitos y condiciones que deban reunir los bancos de datos en materia de seguridad, así como otras medidas técnicas necesarias para el debido tratamiento de los datos.

Finalmente, cabe observar que a pesar de que la legislación peruana en materia de protección de datos personales ha sido objeto de actualizaciones recientes, como la que se llevó a cabo en el año de 2017, no introdujo en su texto los términos adoptados por el RGPD y los instrumentos internacionales modernizados. Sin embargo, esta legislación adopta criterios generales que abren las puertas para su posterior desarrollo a través de mecanismos regulatorios por parte de la Autoridad Nacional de Protección de Datos.

Consideraciones finales y conclusiones

En este artículo hemos analizado cuatro enfoques bajo los que se aborda la interacción entre la legislación de competencia y la de protección de datos. La interacción entre ambas políticas es compleja, no cuenta con un cuerpo de antecedentes y adquiere diferentes formas. Si bien los enfoques analizados pueden lucir irreconciliables entre sí, su validez y aplicabilidad es un resultado en función de cada caso. El enfoque de legislaciones en tensión se vincula directamente con el poder de mercado que los datos pueden conferir a la empresa que los posee. De esta manera la tenencia de datos puede implicar ventajas competitivas y su negativa, prácticas exclusorias. La tensión surge frente a obligaciones de acceso a los datos. El enfoque de privacidad implica incluir consideraciones de impacto en la privacidad y protección de datos con el objetivo de evitar prácticas explotativas. La evidencia sobre la interacción y aplicación de los distintos enfoques es aún incipiente, sobre todo en la región. Esto muestra que la problemática se encuentra todavía en una etapa inicial que merece continuar con su estudio y seguimiento.

Para el análisis de la interacción entre la competencia económica y la privacidad y la protección de datos personales es necesario tomar en consideración que aún existen diferencias significativas en los estándares de protección de datos personales adoptados por los países de la región. Si bien existe una tendencia creciente a elevar los estándares de protección de datos personales, bajo la influencia del RGPD de la Unión Europea, la legislación doméstica en Latinoamérica y el Caribe e, incluso, los instrumentos internacionales que contemplan este derecho presentan diferencias sustantivas entre sí. Los diferentes estándares afectan la implementación del enfoque de privacidad, en la medida en que el estándar orienta a la agencia de competencia para evaluar si hay comportamientos explotativos.

En el ámbito internacional, el análisis comparado realizado de diversos instrumentos internacionales, a partir de la previa selección de indicadores relativos a los principios, obligaciones y el régimen aplicable a las categorías especiales de datos, lleva a concluir que los Estándares Iberoamericanos de Protección de Datos Personales, elaborado por la Red Iberoamericana de Protección de Datos, son los que mayor cercanía presentan con el RGPD, aún por encima de las similitudes que presenta el Convenio 108+ del Consejo de Europa. Este hallazgo resulta significativo si consideramos que ese instrumento internacional de *soft law* pretende guiar el diseño normativo de la protección de datos personales en los países de la región, con el objeto de generar estándares comunes.

En el ámbito nacional, el análisis comparativo de las legislaciones vigentes en materia de privacidad y protección de datos personales en Argentina, Brasil, Chile, Colombia, El Salvador, México y Perú, frente al RGPD, permite concluir que México es el país que mayor cercanía presenta con el modelo de la Unión Europea, específicamente por lo que hace a su legislación aplicable para el sector público. Por su parte, El Salvador es el país que presenta más diferencias, dado su modelo regulatorio sectorial en la materia. Estos hallazgos son consistentes con los distintos niveles de exigencia de los instrumentos internacionales, toda vez que la elaboración de los Estándares Iberoamericanos de Protección de Datos Personales se llevó a cabo durante la presidencia de México en la Red Iberoamericana de Protección de Datos.

Estas diferencias en los países de la región podrían llegar a suponer un distanciamiento entre sus respectivas políticas de competencia económica, especialmente bajo el enfoque que incorpora la privacidad y la protección de datos personales como factores de análisis para evaluar posibles conductas anticompetitivas o de control preventivo para el caso de concentraciones. A todo lo cual se añaden los diferentes costos que implicaría para los agentes económicos (como responsables o encargados del tratamiento de datos personales) cumplir con las disposiciones de la legislación de protección de datos personales, donde un mayor nivel de obligaciones supone un incremento en los costos. La interacción entre ambas legislaciones ha mostrado cierta evolución en el tiempo, como así también diferentes voces en relación con cómo debe implementarse dicha interacción. La complejidad de la interacción, puesta en evidencia a lo largo de este documento, lleva a formular una serie de lineamientos preliminares.

La comunicación y cooperación entre agencias de competencia y protección de datos aparece como un componente indispensable para el despliegue de intervenciones con impactos pro-competitivos y beneficiosos para los usuarios. La normativa condiciona la manera en que esta comunicación puede ser llevada a cabo y en algunos casos podría erigirse como una barrera a la misma. Medidas posibles de ser implementadas en el corto plazo y que no implican cambios de normativas incluyen:

1. puesta en común de la problemática que permita identificar puntos de encuentro para guiar el accionar cotidiano de ambas agencias a la hora de abordar casos de la economía digital;

2. intercambio de capacitaciones a profesionales de cada agencia sobre fundamentos de las legislaciones; i.e., los técnicos de la agencia de competencia deberían adquirir nociones de la legislación de protección de datos local y los técnicos del organismo de protección de datos conocimiento de la legislación de competencia local;

3. identificación de situaciones de riesgo que cada agencia debería reportar a la otra, lo suficientemente concretas para que las agencias no se recarguen de trabajo innecesario mutuamente.

El entorno digital supone retos compartidos, por lo que la necesidad de generar espacios de colaboración y cooperación entre las autoridades de competencia económica y protección de datos personales requiere de una atención en el ámbito nacional, regional y global. El acercamiento a través de instituciones, organismos y redes internacionales en ambas materias podría resultar favorable para alcanzar estos objetivos y generar directrices que permitan armonizar políticas compatibles con la economía digital y las necesidades de las sociedades interconectadas.

Referencias

Abarca, M. (2021), Incipient Digital Markets: Insights from Chilean Case Law, Competition Policy International, Latin America Column.

Athey, S., Catalini, C. & Tucker, C. (2017), The Digital Privacy Paradox: Small Money, Small Costs, Small Talk, https://www.nber.org/papers/w23488.

Benussi, Carlo (2020), Obligaciones de seguridad en el tratamiento de datos personales en Chile: escenario actual y desafíos regulatorios pendientes, Revista Chilena de Derecho y Tecnología, vol. 9, núm. 1, pp. 227-279.

Botta, M. & Wiedemann, K. (2019), Exploitative Conducts in Digital Markets: Time for a Discussion after the Facebook Decision, Journal of European Competition Law & Practice, 10, 8, pp. 467.

Califano, B. (2021), 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 (CELE) Universidad de Palermo, febrero de 2021. https://www.palermo.edu/Archivos_content/2021/cele/datos-personales-argentina-ecuador/Datos-personales-Argentina-y-Ecuador.pdf

CMA-ICO (2021), CMA-ICO joint statement on competition and data protection law, Policy Paper.

COFECE (2018), Repensar la competencia en la Economía Digital https://www.cofece.mx/wp-content/uploads/2018/03/repensarlacompetenciaenlaeconomiadigital_01022018.pdf

Council of Europe (2018), Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, January 28, 2018. https://rm.coe.int/16800ca434

Costa-Cabral and Lynskey (2017), Family ties: the intersection between data protection and competition in EU Law, Kluwer Law International. Common Market Law Review, 54 (1), pp. 11-50.

Facuse, V. (2020), seminario Competencia, Privacidad y Datos Personales del capítulo América Latina de ASCOLA y la Asociación Colombiana de Datos y Privacidad – ADAPRI, https://lalibrecompetencia.com/2020/09/25/video-del-seminario-competencia-privacidad-y-datos-personales/.

FNE (2021) Guía para el Análisis de Operaciones de Concentración Horizontales

Gal, M. & Aviv, O. (2020), The Competitive Effects of the GDPR, Journal of Competition Law and Economics, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3548444.

Greco, E. & Viecens, M.F. (2021), Economía digital en América Latina: ¿y dónde están las fusiones? Reflexiones para la región, de próxima publicación.

Liguori, L. Marasá, E. & Picciano, I. (2021), Data Privacy and Competition Protection in Europe: Convergence or Conflict?, Competition Policy International, Europe Column.

Mantelero, Alessando (2021), The future of data protection: Gold Standard vs. global standard, Law & Security Review, vol. 40, April 2021. https://www.sciencedirect.com/science/article/abs/pii/S0267364920301059

Mariscal, E. & Elbittar, A. (2019), Pride and prejudice: investigations and mergers in digital markets from a developing world´s viewpoint, Competition Policy International Antitrust Chronicle, August.

Marthews & Tucker, C. (2019), Privacy policy and competition, https://www.brookings.edu/wp-content/uploads/2019/12/ES-12.04.19-Marthews-Tucker.pdf.

Martínez, E. (2020), Marco regulatorio de autoridades de protección de datos personales en Iberoamérica. Un estudio comparado 2020, AECID, Embajada de España en Colombia. https://www.redipd.org/sites/default/files/inline-files/marco-regulatorio-autoridades-protección-datos-personales-iberoamerica-un-estudio-comparado-2020%20_0.pdf

Noguera, A. M. (2020), seminario Competencia, Privacidad y Datos Personales del capítulo América Latina de ASCOLA y la Asociación Colombiana de Datos y Privacidad – ADAPRI, https://lalibrecompetencia.com/2020/09/25/video-del-seminario-competencia-privacidad-y-datos-personales/.

OECD (2020a) Consumer data rights and competition, https://www.oecd.org/daf/competition/consumer-data-rights-and-competition.htm, just to mention some of the OECD documents on this topic.

OCDE (2020b) Roundtable on Conglomerate Effects of Mergers,

OECD (2016), Big data: bringing competition policy to the digital era, https://one.oecd.org/document/DAF/COMP(2016)14/en/pdf;

OECD-Colombia (2020), Consumer data rights and competition – Note by Colombia, https://one.oecd.org/document/DAF/COMP/WD(2020)42/en/pdf.

OECD-México (2020), Consumer data rights and competition – Note by Mexico (IFT), https://one.oecd.org/document/DAF/COMP/WD(2020)37/en/pdf.

OECD (2013), The OECD Privacy Framework, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

Olivos, Milagros (2020), El derecho a la protección de datos personales en el Perú: 27 años desde su incorporación en la Constitución Política de 1993", Ius: Revista de investigación de la Facultad de Derecho, vol. 9, núm. 1, Universidad Católica Santo Toribio de Mogrovejo, pp. 83-100.

Palacios, A. (2021), Competition Tools for Digital Markets in Mexico: Section 94 of the Economic Competition Federal Act, Competition Policy International, https://www.competitionpolicyinternational.com/competition-tools-for-digital-markets-in-mexico-section-94-of-the-economic-competition-federal-act/.

Prince, J. & Wallsten, S. (2020) How Much is Privacy Worth Around the World and Across Platforms?, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3528386.

Robertson, V. (2020), Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data, 57 Common Market Law Review, 161–189.

Tucker, C. E. (2020), Digital Data as an Essential Facility: Control, Competition Policy International.

CENTRO
LATAM
DIGITAL

Centro LATAM Digital
Centro de Política Digital para América Latina, A.C.
Ciudad de México, CDMX, México

@LATAMxDigital | www.centrolatam.digital