2025

Empresas y Servicios en la Nube: El Desafío Jurídico de los Datos y la Conexidad en Contratos Tecnológicos

ESPECIALIZACIÓN EN DERECHO DE LA EMPRESA
FCJS (UNL) COHORTE 2022
ELIANA MARICEL PISACCO

Tabla de contenido

1.Introducción

Vivimos en una era en la que los datos constituyen uno de los activos más valiosos del entorno económico y empresarial. Las empresas tecnológicas, en particular, se han convertido en verdaderas arquitectas del ecosistema digital, desarrollando modelos de negocio centrados en la recopilación, procesamiento y transferencia de grandes volúmenes de datos. En este escenario, los servicios en la nube (cloud computing) han adquirido un rol protagónico, al permitir el almacenamiento, análisis y circulación de información a una escala y velocidad sin precedentes. Esta dinámica se inscribe dentro de lo que algunos autores han denominado la sociedad de la transparencia[1], un nuevo paradigma en el que se promueve la visibilidad total de la información, a menudo bajo la promesa de eficiencia, control y seguridad, pero que también conlleva riesgos asociados a la exposición, la vigilancia y la erosión de ciertos derechos fundamentales, como la privacidad.

Esta transformación tecnológica genera una serie de oportunidades, pero también múltiples desafíos jurídicos, especialmente cuando los datos personales se transfieren entre distintas empresas. Si bien el marco normativo en materia de protección de datos ha avanzado tanto a nivel nacional como internacional, subsisten importantes interrogantes sobre la forma en que se distribuyen los riesgos legales y contractuales entre los distintos actores que intervienen en el tratamiento y resguardo de la información.

Un caso paradigmático que expuso las consecuencias de una inadecuada gestión de datos personales fue el escándalo de Cambridge Analytica[2], en el que se evidenció la facilidad con la que información sensible puede ser recolectada, transferida y utilizada sin un consentimiento válido ni transparencia en el tratamiento. Si bien este trabajo no se propone analizar en profundidad aquel caso, su mención sirve como punto de partida para comprender la gravedad del problema y su relevancia actual.

En este contexto, el presente trabajo tiene como objetivo analizar los criterios jurídicos que rigen la transferencia de datos entre empresas, con especial énfasis en la asignación de responsabilidades en los contratos de servicios en la nube. A partir de un enfoque centrado en la contratación entre empresas (B2B), se pretende comprender cómo se distribuyen las obligaciones en materia de protección de

[1] Han, B-C. (2013). La sociedad de la transparencia.
[2] BBC News Mundo. (2019). Cambridge Analytica: la multa récord que deberá pagar Facebook por la forma en que manejó los datos de 87 millones de usuarios. BBC Mundo. https://www.bbc.com/mundo/noticias-49093124

datos, qué modelos de responsabilidad se utilizan actualmente y cuáles son los límites de esta distribución en función del orden público y los derechos fundamentales involucrados.

Para cumplir con este objetivo, se desarrollará primero un marco teórico que aborde los principales conceptos asociados a los diferentes tipos de datos, que es el modelo de negocio del "cloud computing" y los principales proveedores de servicios en la nube. Luego se describirán los distintos tipos de servicios en la nube —SaaS, PaaS, IaaS—, su funcionamiento y el marco normativo de la protección de datos. Posteriormente, se analizará cómo los contratos celebrados entre empresas proveedoras de servicios en la nube contemplan (o no) cláusulas de limitación de responsabilidad, distribución de riesgos y mecanismos de cumplimiento normativo, así como la posibilidad de extender la responsabilidad a otras partes de la cadena contractual. Finalmente, se formularán algunas propuestas de mejora orientadas a fortalecer la seguridad jurídica en el uso de tecnologías en la nube y a resguardar los derechos fundamentales de las personas cuyos datos son objeto de tratamiento.

Este trabajo se basa en el análisis de normativa nacional e internacional (como el RGPD europeo, la Ley 25.326 argentina, disposiciones de la Dirección Nacional de Protección de Datos Personales (DNPDP) y Agencia de Accenso a la Información Pública (AAIP), proyectos de ley, etc.), jurisprudencia relevante y doctrina especializada, con el propósito de contribuir a una reflexión crítica sobre los desafíos jurídicos B2B.

2. Marco Teórico y Conceptual

2.1 Empresas y economía de los datos

2.1.1 El dato como activo digital.

El derecho a la protección de datos personales es el derecho fundamental que tiene la persona a controlar el uso que se hace de la información que personalmente le concierne, para evitar o rechazar usos que puedan perjudicarle. Se considera Datos a *"Información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho"* (Diccionario de la lengua española, 2025).

Tanto los datos en general como los datos personales, cumpliendo ciertas condiciones sirve a las empresas como activos digitales. La principal ventaja radica en que los datos tienen un valor económico ya que son utilizados para generar ingresos, tomar decisiones o mejorar procesos.

Los datos protegidos se clasifican en las siguientes categorías:

- **Datos personales**: *toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona*[3]*;*
- **Datos sensibles:** *Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual*[4]
- **Datos biométricos:** *datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos*[5]*;*
- **Datos genéticos**: *datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona* (Unión Europea, 2016).
- **Datos relativos a la salud:** *datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud* (Unión Europea, 2016).

2.1.2 La Intimidad y Privacidad como Derechos Personalísimos

Como correlato de la protección de los datos personales, la protección de la intimidad consiste en mantener inviolada la propia esfera de la vida íntima, especialmente en una sociedad marcada por la tecnología donde todo se vuelve objeto de información. La fundamentación jurídica del derecho a la protección de datos personales debe relacionarse con el tradicional derecho a la intimidad o a la vida privada, pero lo excede.

La incorporación de los tratados sobre derechos humanos en la Constitución Nacional ha cobrado particular importancia en lo que respecta a los derechos personalísimos como son los derechos que el hábeas data recepta. Algunos autores consideran el hábeas data como un derecho humano de tercera generación que surge ante la necesidad de una protección adecuada de la privacidad frente al avance desproporcionado de las tecnologías de la información. El Pacto de San José de Costa Rica (Convención Americana sobre Derechos Humanos)[6], en su Artículo 11 sobre la Protección de la Honra y de la Dignidad establece que nadie puede ser objeto de

[3] (Unión Europea, 2016)
[4] (Ley 25.326, 2000)
[5] (Unión Europea, 2016)
[6] (Organización de los Estados Americanos, 1969)

injerencias arbitrarias o abusivas en su vida privada. Este derecho a la intimidad o privacidad conlleva la imposibilidad de injerencias no solo de otras personas sino también del Estado.

Tal enfoque ha sido reafirmado por la jurisprudencia, como se observa en el caso Halabi, Ernesto c/ P.E.N. – ley 25.783 – dto. 1563/04 s/ amparo ley 16.986[7]. Ernesto Halabi interpuso una acción de amparo contra el Poder Ejecutivo Nacional, cuestionando la constitucionalidad de la ley 25.873 y su decreto reglamentario 1563/04. La ley y el decreto autorizaban la intervención de las comunicaciones telefónicas y por Internet. Esta normativa, a requerimiento judicial o del Ministerio Público, permitía el conocimiento de los contenidos de las comunicaciones de los usuarios, incluso si no estaban involucrados en delitos. Además, imponía a las empresas la obligación de registrar y conservar los contenidos de tales comunicaciones durante diez años. Halabi consideró que estas disposiciones vulneraban los derechos establecidos en los artículos 18 y 19 de la Constitución Nacional.

Tanto en primera como en segunda instancia se declaró la inconstitucionalidad de la norma cuestionada. El Estado nacional dedujo un recurso extraordinario, llevando el caso a la Corte Suprema de Justicia de la Nación (CSJN). La CSJN, por mayoría, declaró la inconstitucionalidad de la ley 25.873 en lo relativo a la autorización de la intervención de comunicaciones telefónicas y por Internet y la obligación de las empresas de preservar la información sobre las comunicaciones de los usuarios por diez años. Los magistrados de la Corte entendieron que "las comunicaciones a las que se refiere la mencionada ley integran la esfera de la intimidad de las personas y se encuentran protegidas por los artículos 18 y 19 de la Constitución Nacional". Esto subraya la conexión directa entre las comunicaciones (y los datos derivados de ellas) y el derecho fundamental a la intimidad.

En resumen, la protección de datos personales es un derecho fundamental reconocido, distinto del derecho a la intimidad y la privacidad, aunque estrechamente relacionado[8]. Mientras la intimidad protege una esfera reservada de la vida privada, la protección de datos se refiere al control que una persona tiene sobre cualquier dato que la identifique. La privacidad puede ser vista como un concepto más amplio que abarca tanto la intimidad como la protección de datos. La violación de la protección de datos puede, en ocasiones, derivar en una violación de la intimidad.

2.1.3 Modelos de negocio basados en datos y servicios en la nube.

Uno de los modelos de negocios basados en datos son los servicios de computación en la nube o 'cloud computing'. La principal ventaja de este modelo de negocio es la

[7] (Halabi, Ernesto c/ P.E.N. – ley 25.783 – dto. 1563/04 s/ amparo ley 16.986, 2008)
[8] (Marzo, 2018)

reducción de costos ya que se puede contratar a demanda. Ello es así porque los recursos de tecnología informática en la Nube no se almacenan localmente en los dispositivos personales de los usuarios, sino que se acceden a ellos a través de una red distribuida[9].

Aller Fernández[10] menciona las cinco características que definen el cloud computing:

- **Autoservicio**: el usuario puede utilizar más capacidades de procesamiento o almacenamiento de la información, sin pedirlo expresamente al proveedor del servicio.

- **Amplio acceso a la Red**: se puede acceder a ésta desde diferentes dispositivos y redes.

- **Agrupación y reserva de recursos**: hay un conjunto de recursos compartidos por los usuarios, de acuerdo con sus necesidades puntuales, que implica que en cada momento los recursos reservados puedan ser diferentes.

- **Rapidez y elasticidad**: se puede acceder a los nuevos recursos de manera inmediata y aparentemente ilimitada.

- **Servicio medible y supervisado**: se controla el uso y en todo momento se puede conocer, de manera transparente, el nivel de recursos utilizado.

2.1.4 Principales actores en el modelo de negocio de cloud computing

Este modelo de negocio implica la intervención de diversos actores, tales como: **el Responsable del Tratamiento (RT)** y el **Encargado del Tratamiento (ET)**. El RT es aquella persona humana o jurídica, pública o privada, que decide sobre la finalidad y los medios del tratamiento de los datos personales. Es decir, quien posee la base de datos y determina su uso. Por su parte, el ET es quien trata los datos por cuenta del responsable, típicamente un tercero, como lo es una empresa proveedora de servicios en la nube.

La distribución de estos roles no solo determina competencias técnicas, sino que también implica una asignación diferenciada de obligaciones y responsabilidades. Cada parte debe cumplir con estándares específicos de seguridad, confidencialidad y legalidad en el tratamiento de la información, conforme a las exigencias de la normativa. Muchas veces, las normas, resultan insuficientes en cuanto al detalle técnico sobre cómo deben implementarse las medidas de seguridad. En este punto, adquieren especial relevancia los estándares internacionales, como la serie de normas ISO/IEC 27000, orientadas a la gestión de la seguridad de la información. Dentro de esta serie,

[9] (Compagnucci, 2022)
[10] (Aller, 2012)

las normas ISO/IEC 27018 y ISO/IEC 27002 se presentan como guías complementarias ampliamente aceptadas en el sector empresarial.

Estas certificaciones, además de establecer buenas prácticas, funcionan como mecanismos de autorregulación técnica que otorgan a las empresas proveedoras de servicios en la nube una ventaja competitiva. La adopción de tales estándares refuerza la confianza de los clientes corporativos al demostrar el compromiso de las empresas tecnológicas con la protección de los datos personales y el cumplimiento normativo.

2.2 Principales proveedores de servicios en la nube

2.2.1 Comparación de las principales plataformas proveedoras de servicios en la nube

Hay en la actualidad tres actores principales en la industria de servicios de cloud: Amazon (AWS), Microsoft (Azure) y Google (GCP). Su destacada presencia en otros ámbitos de la economía digital les da, además, una ventaja competitiva sobre sus rivales en el sector cloud, ya que gozan de amplias bases de datos de clientes (lo que les permite beneficiarse de significativos efectos de red), y pueden aprovechar las economías de escala y alcance ligadas a los variados servicios que ya ofrecen dentro de sus propios ecosistemas.

AWS ofrece una amplia gama de servicios para servicios de gran escala, un alcance global, escalabilidad y una gran experiencia en el mercado, Azure proporciona una integración perfecta con las tecnologías de Microsoft, ofreciendo sólidas capacidades de servicios de tecnología en la nube híbrida y GCP se destaca por su rendimiento, baja latencia y sus servicios avanzados de analítica de datos e inteligencia artificial[11].

2.2.2 Contratos de servicios en la nube (SaaS, PaaS, IaaS).

De acuerdo con la clasificación presentada por Aller Fernández, existen diferentes tipos de nubes:

- **nubes públicas**: se trata de aquellas que son administradas por el proveedor del servicio. La gran ventaja es que no requieren de una inversión inicial para comenzar a utilizarlas y no suponen un gasto de mantenimiento para el cliente. Estas nubes son compartidas con otros clientes dentro de los data centers del proveedor.
- **nubes privadas**: las nubes privadas, a diferencia de las públicas, son administradas por el cliente para obtener un mayor control. Debido a esto, supone una inversión inicial en la infraestructura ya que esta será alojada en las instalaciones del cliente.

[11] (Petersen, 2024)

- **nubes comunitarias:** se dan cuando dos o más organizaciones forman una alianza para implementar una infraestructura cloud orientada a objetivos similares y con un marco de seguridad y privacidad común.
- **nubes híbridas**: Esta opción es intermedia entre la pública y la privada. la idea principal de las mismas es que el cliente podrá mantener el control de aquellas aplicaciones principales y delegar la administración en las que considere secundarias.

Hasta la fecha, los ecosistemas cloud se estructuran habitualmente en torno a tres servicios básicos:

- **Infraestructura como servicio (IaaS, por sus siglas en inglés):** Este tipo de servicio ofrece la infraestructura necesaria para poder subir nuestro entorno y además ejecutar el software propietario en ella. Los dos pilares fundamentales son la computación y el almacenamiento como servicio, es decir, el alquiler de espacio de alojamiento o cloud hosting.
- **Plataforma como servicio (PaaS):** cuando hablamos de la plataforma dentro de la nube nos ofrecen el entorno donde podemos desplegar directamente nuestras aplicaciones, es decir, alquiler de plataformas para desarrolladores.
- **Software como servicio (SaaS):** es el servicio transformado en aplicación final proporcionado por el proveedor, listo para ser usado por los clientes. En este tipo de servicio se nos asegura el mantenimiento, el soporte y la disponibilidad del programa de ordenador.

En función del estadio de desarrollo en que un cliente ha adoptado servicios cloud, podemos distinguir entre dos categorías:

- Empresas que contratan el uso de servicios cloud para toda o parte de su operativa en las que la infraestructura informática sigue estando físicamente en la sede de la empresa (on-premises);
- Empresas cuyas infraestructuras informáticas se han desarrollado directamente en y desde la nube (cloud-native companies)[12].

2.3 Protección de datos personales en entornos empresariales

2.3.1Marco normativo relevante:

La protección de datos en Argentina se encuentra en la esencia de su ordenamiento jurídico, remontándose al derecho a la privacidad implícito en el Artículo 19 de la Constitución Nacional (CN). La reforma constitucional de 1994 estableció expresamente el derecho sobre los datos personales en el Artículo 43 de la CN.

[12] (Estella, 2024)

Desde el año 2000, existe la ley 25.326 de Protección de Datos Personales que regula la herramienta del Habeas Data, junto con su decreto reglamentario (Decreto 1558/2001). Tambien establece que cuando se quieran tratar datos personales se debe dar cumplimiento a una serie de obligaciones que permitirán que dicho tratamiento sea legal:

—Obtener los datos mediante medios lícitos y para fines lícitos (arts. 3º y 5º).

—Brindar seguridad a esos datos (art. 9º y res. 47/2018, AAIP).

—Utilizar esos datos para los fines por los que fueron recopilados (art. 4º).

—Brindar los derechos ARCO (Acceso, Rectificación, Cancelación, Oposición) a sus titulares (art. 4º).

—Inscribir las Bases de Datos (art. 3º).

La ley se divide en capítulos:

1. El primer capítulo aborda las disposiciones generales, estableciendo el propósito de la ley en su artículo 1 y ofreciendo, en el artículo 2, definiciones clave que facilitan su correcta interpretación.
2. El segundo capítulo se centra en los principios fundamentales de la protección de datos, destacando la legalidad en el tratamiento y la calidad de los datos. Esto implica que la información debe ser veraz, precisa, pertinente, actualizada y adecuada en relación con los fines para los que se recopila. Asimismo, se contemplan principios como la obtención leal de los datos, la determinación específica de su finalidad, la restricción del uso en función de ese fin, y la limitación temporal del almacenamiento. También se incluyen la confidencialidad, el tratamiento especial de los datos sensibles, la seguridad en el tratamiento, y las reglas sobre cesión y transferencias internacionales de datos, todos ellos destinados a proteger los bienes jurídicos que la ley resguarda.
3. El tercer capítulo aborda los principios vinculados a los derechos de las personas titulares de los datos.
4. El cuarto capítulo, por su parte, regula las obligaciones de los usuarios y responsables de archivos, registros y bases de datos.

Estos primeros cuatro capítulos tienen carácter de orden público, según lo indica la propia ley, lo cual conlleva implicancias jurídicas relevantes.

5. El quinto capítulo se dedica al organismo encargado de supervisar el cumplimiento de esta normativa, así como a los códigos de conducta aplicables.

6. En el sexto capítulo se detallan las sanciones administrativas y penales por incumplimiento de la ley.
7. Finalmente, el séptimo capítulo establece el marco normativo para la acción de protección de los datos personales.

Lo hasta aquí señalado, permitió que Argentina sea considerada como país de protección adecuada por la Unión Europea (UE). Este punto resulta sumamente importante pues facilita nada más y nada menos que la tan necesaria transferencia internacional de datos (Abdelnabe Vila, 2020).

Sin embargo, en lo que respecta a los servicios de almacenamiento en la nube no hay una norma dentro de la actual ley que haga referencia a ello. Podemos interpretar a través del juego de los arts. 9,10 y 25 los criterios aplicables a este tipo de contratos. El articulo 9 legisla sobre la seguridad de los datos personales, el RT del banco de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad e integridad de los datos personales. El artículo 10 se legisla sobre el deber de confidencialidad de los datos personales. La confidencialidad hace referencia a que los datos personales no puedan estar disponibles o ser descubiertos por personas, entidades o procesos no autorizados. Y, en el artículo 25 se introduce la figura del ET: "*es aquél que presta servicios de procesamiento de datos por encargo del responsable de una base de datos*"

Tambien a nivel nacional hay diversas Resoluciones y disposiciones de la AAIP y la DNPDP que complementan la ley, como la Resolución 40/2018 sobre Política Modelo y Delegado de Protección de Datos, la Resolución 47/2018 sobre Medidas de Seguridad, la Resolución 43/2019 que la lista de países con protección adecuada y el régimen de Normas Corporativas Vinculantes (BCRs) y la Disposición 60/2016 mediante la cual se establecen dos modelos de contratos de transferencia internacional de datos a países con legislación no adecuada que, en caso de utilizarse no requieren someterse a aprobación de la autoridad. Asimismo, se dispone —a modo de lista blanca— la lista de países considerados por Argentina con adecuada protección de datos personales.

Por último, cabe resaltar que a nivel nacional que ha habido múltiples proyectos de Ley para actualizar la Ley de Protección de Datos Personales, ya sea incluyendo conceptos más amplios que los previstos actualmente o para ajironarlo a las nuevas tecnologías, sin embargo, la mayoría de estos proyectos han perdido estado parlamentario. El último proyecto de Ley fue la comunicación 0087/23 del Poder Ejecutivo enviada a la Cámara de Diputados en junio 2023 y que obtuvo media sanción en agosto 2024. Para la elaboración del proyecto, la Agencia de Acceso a la Información Pública (AAIP) tomó como referencia diversos estándares y normativas internacionales y regionales, incluyendo el Reglamento General de Protección de Datos (RGPD), el Convenio 108 del

Consejo de Europa y su versión modernizada (Convenio 108+), estándares de la Red Iberoamericana de Protección de Datos (RIPD), y legislaciones de otros países.

Entre los contenidos más importantes que incorpora el proyecto de ley se destacan:

•Regulación de las transferencias internacionales de datos. Establece tres mecanismos principales para legitimar los flujos transfronterizos: decisiones de adecuación, mecanismos que ofrezcan garantías adecuadas (como cláusulas contractuales o normas corporativas vinculantes) y excepciones (bajo ciertas condiciones, no de manera habitual o periódica).

•Ampliación de los derechos de los titulares de los datos. Además de los derechos ya existentes (acceso, rectificación, oposición, supresión -conocidos tradicionalmente como derechos ARCO) el proyecto incorpora nuevos derechos: el derecho a la limitación del tratamiento y derechos sobre las decisiones automatizadas y la elaboración de perfiles.

•Endurecimiento del régimen de procedimientos y sanciones. El proyecto eleva sustantivamente los montos de las multas, que estaban desactualizados (mil a cien mil pesos en la ley de 2000). Además, incorpora una unidad móvil sujeta a la variación del Índice de Precios al Consumidor para mantener actualizados los valores de las sanciones.

A nivel Internacional el RGPD es un reglamento europeo, adoptado en 2016 y efectivo en 2018. Es un instrumento jurídicamente vinculante en el ámbito de la protección de datos, de aplicación directa en todos los Estados Miembros de la UE. Se considera un hito que exacerbó el régimen de protección de datos existente y ha servido como modelo e inspiración para otras leyes en la región y el mundo, mostrando una tendencia a homogeneizar la protección de datos a nivel iberoamericano.

Una de sus características más relevantes y comentadas es su alcance que excede la UE. El RGPD se aplica al tratamiento de datos personales en el marco de las actividades de un establecimiento en la UE, independientemente de si el tratamiento tiene lugar en la Unión o no. Además, se aplica a RT o ET no establecidos en la UE si sus actividades de tratamiento se relacionan con la oferta de bienes o servicios a interesados en la Unión o el seguimiento de su comportamiento dentro de la Unión.

Además de los derechos tradicionalmente reconocidos (como acceso, rectificación, supresión/cancelación y oposición - los derechos ARCO), incorpora nuevos derechos:

- Derecho a la limitación del tratamiento.

- Derecho a no ser objeto de decisiones basadas únicamente en tratamientos automatizados, incluida la elaboración de perfiles (profiling).
- Derecho a la portabilidad de los datos. Este es especialmente relevante, particularmente en el entorno del cloud computing, permitiendo al interesado obtener sus datos en un formato estructurado y de uso común o transmitirlos directamente a otro responsable, si es técnicamente posible. Aunque es un derecho del interesado (persona física) y no del cliente en una relación B2B (empresa), requiere la cooperación del proveedor/encargado para ser efectivo en la nube.

Establece obligaciones más detalladas para el encargado, incluyendo la necesidad de un **contrato por escrito** que especifique la materia, duración, naturaleza, fines, tipo de datos, categorías de interesados, y obligaciones de las partes, así como asistencia al responsable.

Promueve la responsabilidad proactiva (accountability), que implica la adopción de medidas internas y procesos para cumplir con la normativa, incluyendo la realización de Evaluaciones de Impacto de Protección de Datos (EIPD) para tratamientos de alto riesgo.

Requiere la implementación de medidas de seguridad técnicas y organizativas adecuadas al riesgo, y establece un régimen de notificación de violaciones de seguridad (data breaches) a la autoridad de control y, en ciertos casos, a los interesados.

Regula de forma detallada las transferencias de datos personales a países fuera de la UE (terceros países). El principio general es que solo se permiten si el país tercero garantiza un nivel de protección adecuado. En ausencia de una decisión de adecuación de la Comisión, las transferencias requieren garantías adecuadas, como las Cláusulas Contractuales Tipo (SCCs) o las Normas Corporativas Vinculantes (BCRs) para transferencias dentro de grupos empresariales, asegurando que los interesados cuenten con derechos exigibles y acciones legales efectivas.

A nivel sancionatorio es el más temido por las empresas. Las multas administrativas por incumplimientos pueden alcanzar hasta 20.000.000 EUR o, en el caso de una empresa, una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

Ha actuado como un motor de cambio a nivel mundial en la regulación de la protección de datos personales.

2.3.2 Principios aplicables en el tratamiento de datos entre empresas.

El tratamiento de datos personales entre empresas, plantea importantes desafíos jurídicos y éticos. Por esta razón, tanto la normativa nacional como los instrumentos

internacionales y regionales han ido consolidando un conjunto de principios que deben guiar este tipo de operaciones. El proyecto de Ley de Protección de Datos Personales en Argentina[13], elaborado por la AAIP, retoma y adapta estándares de documentos de referencia como el RGPD de la Unión Europea, el Convenio 108 del Consejo de Europa, los principios de la Red Iberoamericana de Protección de Datos (RIPD), la LGPD de Brasil, la ley ecuatoriana, entre otros. Este enfoque comparado permite establecer un marco sólido y armónico de principios aplicables al tratamiento de datos entre empresas:

- **Principio de licitud, lealtad y transparencia**: Las empresas deben tratar los datos personales de manera legal, justa y transparente para con los titulares. Esto implica no solo cumplir con una base jurídica habilitante (como el consentimiento o un contrato), sino también asegurar que los titulares comprendan con claridad el destino y uso de sus datos.
- **Principio de finalidad**: La transferencia debe responder a fines determinados, explícitos y legítimos. Los datos no pueden ser utilizados posteriormente para objetivos incompatibles con aquellos informados en el momento de su recolección.
- **Principio de minimización de datos**: Solo deben transferirse aquellos datos que sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los cuales se transfieren.
- **Principio de exactitud**: Los datos deben ser exactos y estar actualizados. Las empresas deben adoptar medidas razonables para asegurar que los datos inexactos, teniendo en cuenta los fines del tratamiento, sean rectificados o eliminados oportunamente.
- **Principio de responsabilidad proactiva y demostrada**: Las empresas no solo deben cumplir con la normativa de protección de datos, sino también poder demostrar ese cumplimiento. Esto implica documentar políticas internas, procesos de auditoría, evaluación de impacto y gestión de incidentes.
- **Principio general de las transferencias internacionales**: Cuando los datos se transfieren a otro país o a un proveedor ubicado en una jurisdicción distinta, deben garantizarse niveles adecuados de protección equivalentes a los que establece la normativa del país de origen. Este principio exige mecanismos contractuales, certificaciones o decisiones de adecuación por parte de autoridades competentes.

Estos principios constituyen la base sobre la cual deben diseñarse, negociarse y ejecutarse los contratos entre empresas que impliquen tratamiento o transferencia de datos personales, especialmente cuando están involucrados proveedores de servicios

[13] (Agencia de acceso a la Información Pública, 2023)

en la nube o actores en distintas jurisdicciones. Su cumplimiento no solo reduce riesgos legales, sino que también refuerza la confianza entre partes y con los usuarios finales.

3. Riesgos jurídicos y extensión de la responsabilidad

3.1 Tratamiento de datos entre empresas

3.1.1 Responsabilidades de las partes del contrato cloud computing

Como se mencionó en la sección 2.1.4, se describirán detalladamente las responsabilidades del RT y ET.

Responsable del Tratamiento

El responsable del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, **determina los fines y los medios del tratamiento**. Ser responsable es fundamentalmente la consecuencia fáctica de que una entidad ha decidido tratar datos personales para su propio interés.

En general se le atribuyen las siguientes responsabilidades:

- Es **responsable de cualquier tratamiento de datos personales** realizado por él mismo o por su cuenta.
- Es **responsable del cumplimiento** del reglamento y debe ser **capaz de demostrarlo** ("responsabilidad proactiva"). Esto implica la **implementación de la debida diligencia**.
- Debe aplicar **medidas técnicas y organizativas apropiadas** para garantizar y poder demostrar que el tratamiento es conforme con la normativa. Dichas medidas deben ser útiles, oportunas, pertinentes y eficaces, y proporcionales a las modalidades y finalidades del tratamiento, su contexto, tipo y categoría de datos, y el riesgo para los derechos del titular.
- Debe tener en cuenta la naturaleza, el ámbito, el contexto, los fines del tratamiento y los riesgos para los derechos y libertades de las personas físicas al aplicar medidas. Las medidas deben revisarse y actualizarse cuando sea necesario.
- Debe prever y aplicar medidas tecnológicas y organizativas apropiadas **desde el diseño y antes del tratamiento** para cumplir los principios y garantizar los derechos de los titulares ("protección de datos desde el diseño").
- Debe indicar cuáles son sus **personas autorizadas** para tratar datos personales.
- Debe arbitrar fórmulas para facilitar al interesado el **ejercicio de sus derechos**, incluidos el acceso, rectificación, supresión, limitación, oposición y portabilidad.
- Debe proporcionar medios para que las **solicitudes se presenten por medios electrónicos**.

- Debe **responder a las solicitudes** del interesado sin dilación indebida y, a más tardar, en el plazo de un mes (prorrogable por dos meses más), y explicar sus motivos si no las atiende. Si no satisface los derechos, debe informar al interesado.
- Si la base legal para el tratamiento es el consentimiento y se realizan **cambios sustanciales en las políticas**, debe notificar y obtener una nueva autorización.
- Debe mantener **registros de las actividades de tratamiento** bajo su responsabilidad. El contenido del registro incluye, entre otros: nombre/contacto del responsable (y corresponsable/representante/DPO), fines del tratamiento, categorías de interesados y datos, plazos de supresión (si es posible), descripción general de medidas de seguridad.
- Debe **cooperar con la autoridad de control** que lo solicite en el desempeño de sus funciones.
- Debe evaluar los **riesgos inherentes al tratamiento** y aplicar medidas para mitigarlos.
- Debe garantizar que cualquier persona que actúe bajo su autoridad y tenga acceso a datos personales **solo pueda tratarlos siguiendo instrucciones del responsable**, salvo obligación legal.
- En caso de **violación de la seguridad de los datos personales**, debe notificar a la autoridad de control competente sin dilación indebida.
- Debe **documentar todo incidente de seguridad** que ponga en alto riesgo los derechos de los titulares.
- Debe realizar una **evaluación de impacto relativa a la protección de datos (EIPD)** si un tratamiento entraña un alto riesgo, de manera previa a la implementación. Es obligatoria en casos de evaluación sistemática y exhaustiva (perfiles) con efectos jurídicos o significativos. Debe recabar el asesoramiento del DPO para la EIPD.
- Debe llevar a cabo **consultas con la autoridad de control** en caso de alto riesgo antes del tratamiento (si la EIPD indica que el riesgo no puede mitigarse) o durante la tramitación de medidas legislativas. Al consultar, debe facilitar información como las responsabilidades respectivas (incl. corresponsables y encargados), fines/medios, medidas/garantías, DPO, EIPD. **No puede iniciar el tratamiento hasta que la Autoridad se pronuncie**.
- Debe **designar un Delegado de Protección de Datos (DPO)** en los supuestos requeridos: autoridad pública (excepto tribunales), actividades principales que requieran observación habitual/sistemática a gran escala, o tratamiento a gran

escala de categorías especiales/datos penales. Si no corresponde, debe establecer una persona/área para la función de protección de datos y trámite de solicitudes.

- Debe **publicar los datos de contacto del DPO** y comunicarlos a la autoridad de control.
- Debe garantizar que el DPO **participe de forma adecuada y oportuna** en todas las cuestiones relativas a la protección de datos.
- Debe **respaldar al DPO** en el desempeño de sus funciones, facilitando recursos, acceso y mantenimiento de conocimientos.
- Debe garantizar que el DPO **no reciba ninguna instrucción** respecto a sus funciones y no sea destituido ni sancionado por desempeñarlas.
- El DPO debe **rendir cuentas directamente al más alto nivel jerárquico**.
- Al encomendar actividades de tratamiento a un encargado, debe recurrir únicamente a **encargados que ofrezcan suficientes garantías**. La adhesión del encargado a un código de conducta o certificación puede servir como prueba.
- Debe **formalizar mediante un contrato** u otro acto jurídico la prestación de servicios con el encargado del tratamiento.
- Debe **verificar que los encargados** (y subcontratistas) ofrezcan garantías suficientes antes de contratar.
- Debe **exigir al encargado el respeto a las condiciones de seguridad** y debido tratamiento de la información.
- Debe **cumplir las instrucciones, órdenes o requerimientos** que imparta la Autoridad de Aplicación.
- En el caso de cesiones de datos por organismos públicos, debe **formalizar un acuerdo** con el cesionario (si actúa como responsable). El responsable cesionario queda sujeto a las mismas obligaciones que el cedente; ambos responden ante la Autoridad y el titular.
- Es el **sujeto principal legitimado para recibir, valorar, atender, o impugnar solicitudes** de autoridades gubernamentales. En contratos B2B, el cliente es usualmente el principal responsable de atender estas solicitudes.
- Debe ser capaz de **demostrar la existencia del interés legítimo** para el tratamiento, la necesidad de los datos y los criterios de razonabilidad/proporcionalidad.

Encargado del Tratamiento

El encargado del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que **trata datos personales por cuenta del responsable del tratamiento**. En el ámbito del Cloud Computing, el proveedor de servicios se configura típicamente como un encargado del tratamiento. Su rol se limita a cumplir con las instrucciones del responsable.

Las fuentes le atribuyen las siguientes responsabilidades:

- La prestación de servicios debe quedar **formalizada mediante un contrato** por escrito con el responsable. Dicho contrato o acto jurídico estipulará el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos y categorías de interesados, y las obligaciones y derechos del responsable. No requiere el consentimiento del titular.
- Debe **tratar los datos personales únicamente siguiendo instrucciones documentadas del responsable**.
- Los datos personales objeto de tratamiento deben aplicarse o utilizarse con el **fin que figure en el contrato**.
- Debe garantizar que las personas autorizadas para tratar datos personales se hayan **comprometido a respetar la confidencialidad** o estén sujetas a una obligación de confidencialidad. Esta obligación subsiste aun después de finalizada su relación.
- Debe aplicar **medidas técnicas y organizativas apropiadas** para garantizar un nivel de seguridad adecuado al riesgo. Las medidas deben considerar el estado de la técnica, los costes de aplicación, y la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos. Debe tratar los datos bajo condiciones de seguridad apropiadas para impedir su adulteración, pérdida, acceso o uso no autorizado.
- Debe evaluar los **riesgos inherentes al tratamiento** y aplicar medidas para mitigarlos.
- Debe mantener **registros de todas las categorías de actividades de tratamiento** efectuadas por cuenta de un responsable. El registro debe contener, entre otros: nombre/contacto del encargado (y representante/DPO), de cada responsable por cuya cuenta actúa, categorías de tratamientos realizados por cuenta del responsable, transferencias internacionales (si las hay), descripción general de medidas de seguridad.
- Debe **cooperar con la autoridad de control** que lo solicite en el desempeño de sus funciones.

- Debe garantizar que cualquier persona que actúe bajo su autoridad y tenga acceso a datos personales **solo pueda tratarlos siguiendo instrucciones del responsable**, salvo obligación legal.
- Debe **asistir al responsable** (a través de medidas técnicas y organizativas apropiadas, siempre que sea posible) para que este pueda cumplir con su obligación de responder a las solicitudes de los interesados. Esto incluye asistir en el ejercicio de los derechos de acceso, rectificación o supresión. En caso de solicitudes directas del interesado, debe tramitarlas, notificando al responsable y dando aviso al interesado.
- Debe **ayudar al responsable a garantizar el cumplimiento de las obligaciones** establecidas en materia de seguridad, notificación de violaciones de datos, evaluación de impacto y consulta previa, teniendo en cuenta la naturaleza del tratamiento y la información a su disposición.
- Una vez finalizada la prestación de los servicios de tratamiento, debe, a elección del responsable, **suprimir o devolver todos los datos personales** y suprimir las copias existentes.
- Solo puede **conservar los datos personales si el Derecho de la Unión o de los Estados miembros aplicable (o la ley argentina) le obliga**. En tal caso, deben conservarse debidamente bloqueados en tanto pudieran derivarse responsabilidades de su relación con el responsable (plazo máximo de 2 años según la ley argentina propuesta).
- No recurrirá a **otro encargado (subencargado)** sin la **autorización previa y por escrito** (específica o general) del responsable.
- En caso de autorización general, debe **informar al responsable de cualquier cambio previsto** en la incorporación o sustitución de otros encargados, dando oportunidad de oponerse.
- Cuando recurra a otro encargado, debe **imponerle, mediante contrato, las mismas obligaciones de protección de datos** que las estipuladas entre el responsable y el encargado principal.
- Si el subencargado incumple sus obligaciones, **el encargado inicial seguirá siendo plenamente responsable** ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado.
- Si un encargado **infringe el reglamento al determinar los fines y medios** del tratamiento, será considerado **responsable del tratamiento** respecto a dicho tratamiento.

- Debe **designar un Delegado de Protección de Datos (DPO)** en los mismos supuestos requeridos para el responsable. Si no corresponde, debe establecer una persona/área para la función de protección de datos y trámite de solicitudes.
- Debe **publicar los datos de contacto del DPO** y comunicarlos a la autoridad de control.
- Debe garantizar que el DPO **participe de forma adecuada y oportuna**.
- Debe **respaldar al DPO**, facilitando recursos, acceso y mantenimiento de conocimientos.
- Si no está establecido en la REPÚBLICA ARGENTINA y la ley aplica, debe **designar un Representante** en territorio nacional.
- Debe **cumplir las instrucciones, órdenes o requerimientos** que imparta la Autoridad de Aplicación.
- Debe **informar en el plazo de Ley a la Autoridad de Aplicación y al Responsable** cuando se presenten incidentes de seguridad y existan riesgos.
- Debe desarrollar sus **políticas para el tratamiento de los datos personales** e informar a los titulares.

En resumen, el responsable del tratamiento es el **cerebro** que decide *qué* y *por qué* se tratan los datos, mientras que el encargado del tratamiento es el **ejecutor** que realiza el tratamiento *cómo* le indica el responsable. El responsable mantiene la **responsabilidad última** por la protección de los datos, aunque el encargado tiene obligaciones específicas (como seguridad, confidencialidad, asistencia y cumplimiento de instrucciones) y puede ser considerado responsable si determina fines y medios por sí mismo. La relación entre ambos debe formalizarse mediante un **contrato claro** que delimite sus funciones y responsabilidades.

3.1.2 Cadenas de tratamiento y subencargados del tratamiento de datos.

La cadena de subcontrataciones es un fenómeno que se considera inherente a la naturaleza del cloud computing. Esta cadena, a veces descrita como una "caja negra"[14], permite redimensionar los recursos de la nube de forma dinámica según las condiciones del mercado. Teóricamente, podría ser una cadena sin fin. En este contexto, el proveedor de servicios en la nube suele actuar como el encargado del tratamiento, y cuando subcontrata parte del tratamiento a otra entidad, esta última se convierte en un subencargado.

La realización de tratamientos de datos por cuenta de terceros (encargo del tratamiento), incluyendo la subcontratación, debe estar regulada en un contrato por

[14] (Marzo, 2018)

escrito. Este contrato debe establecer expresamente que el encargado (el proveedor) únicamente tratará los datos conforme a las instrucciones del responsable (el cliente), que no los aplicará o utilizará con fin distinto al pactado, ni los comunicará. El proveedor (encargado) debe imponer al subcontratado (subencargado) las mismas obligaciones de protección de datos que él tiene con el cliente (responsable).

En el contexto de las cláusulas contractuales tipo para transferencias internacionales entre encargado y subencargado, se requiere que el exportador de datos (encargado) mantenga una lista de los acuerdos de subtratamiento celebrados, actualizada anualmente, y la ponga a disposición de la autoridad de control.

El RGPD ha endurecido el régimen jurídico aplicable al encargado del tratamiento, y también ha introducido importantes novedades con obligaciones directas para los encargados en relación con la cadena de subcontrataciones.

3.1.3 Transferencia Internacional de Datos entre empresas

La subcontratación a menudo implica transferencias internacionales de datos, esto ocurre porque los datos pueden almacenarse y procesarse en servidores ubicados en el extranjero y los proveedores a menudo operan y transfieren datos a través de múltiples jurisdicciones.

La regla general en muchas normativas (incluida la Ley argentina 25326 y el RGPD) es que las transferencias solo pueden realizarse si el país u organismo receptor garantiza un nivel de protección adecuado. Según la Ley argentina 25326 (Artículo 12), para que una transferencia internacional sea lícita, el tercero receptor debe estar en una jurisdicción que proporcione una legislación con niveles de protección adecuada o equiparable a la de Argentina.

Si el país de destino no garantiza un nivel de protección adecuado, la transferencia solo puede tener lugar si el exportador ofrece garantías apropiadas al tratamiento de los datos, utilizando alguno de las siguientes herramientas:

- **Normas Corporativas Vinculantes (BCRs - Binding Corporate Rules):** Son políticas de protección de datos personales utilizadas para transferencias dentro de un grupo empresarial o una unión de empresas con actividad económica conjunta a responsables o encargados en terceros países. El GDPR las reconoce. En Argentina, la Resolución 159/2018 AAIP agregó la posibilidad de transferencias internacionales entre empresas del mismo grupo incluso a países no considerados de protección adecuada, invocando este mecanismo.
- **Cláusulas Contractuales Tipo (SCCs - Standard Contractual Clauses):** Son modelos de contratos aprobados por la Comisión Europea o autoridades de control (como lo enunciado en la Disposición 60/16 de la DNPDP) que pueden

servir como garantías adecuadas para transferencias. Son muy importantes en el ámbito del Cloud Computing y para transferencias entre responsables y encargados o entre encargados y subencargados.

En este contexto, y especialmente cuando el tratamiento pueda implicar un alto riesgo para los derechos de los titulares, corresponde al exportador realizar una Evaluación de Impacto en la Protección de Datos (DPIA)[15], a fin de identificar los riesgos específicos y establecer medidas que aseguren el cumplimiento de los principios de legalidad, seguridad y responsabilidad proactiva.

3.2 Responsabilidad de los proveedores de servicios en la nube

3.2.1 Comparación de cláusulas en los contratos de adhesión de los principales proveedores de servicios en la nube

Por regla, las empresas proveedoras de servicios en la nube ofrecen contratos tipo o contratos de adhesión, accesibles a través de sus sitios web. Estos documentos establecen las condiciones generales bajo las cuales se rige la relación con los clientes corporativos, que a menudo se ven obligados a aceptar cláusulas preestablecidas sin posibilidad de negociación. Dado el rol crítico que cumplen estas empresas en el tratamiento de datos personales, resulta relevante analizar las condiciones contractuales que proponen.

En los tres casos, se observa un principio común de que el cliente conserva la propiedad de los datos y asume obligaciones de cumplimiento normativo, aunque varía el grado de colaboración del proveedor. Mientras que AWS y Azure asignan claramente al proveedor la implementación de medidas técnicas y organizativas, Google enfatiza un modelo de responsabilidad compartida. En cuanto a la eliminación y recuperación de datos, Microsoft y Google establecen plazos concretos (90 y 30 días respectivamente), lo que favorece la previsibilidad y el cumplimiento, a diferencia de AWS, que no fija plazos específicos, lo que puede representar un riesgo de incumplimiento o pérdida de datos. Asimismo, las cláusulas de exención de responsabilidad en AWS y Google limitan la posibilidad de reclamar por daños intangibles como la reputación, lo cual puede debilitar los mecanismos de resarcimiento en caso de incidentes de seguridad. En el ámbito de las transferencias internacionales, las tres plataformas se ajustan al marco normativo del RGPD, aunque difieren en su grado de transparencia y control: Google y Azure son más explícitas en la localización geográfica y uso de cláusulas contractuales estándar, mientras que AWS deja mayor margen al cliente, lo que implica una carga adicional de cumplimiento para este último. En suma, las diferencias contractuales, técnicas y operativas entre proveedores exigen una evaluación exhaustiva por parte de

[15] (Red Iberoamericana de Protección de Datos, 2021)

las empresas contratantes, ya que la falta de claridad en roles y medidas puede derivar en vulneraciones normativas y riesgos de sanciones regulatorias.

A continuación, un cuadro comparativo entre los contratos disponibles públicamente de los principales proveedores de servicios en la nube, a fin de identificar similitudes, diferencias y posibles riesgos desde la perspectiva del compliance en protección de datos y asignación de responsabilidades.

Categoría	AWS (Amazon Web Services)[16]	Microsoft Azure[17]	Google Cloud Platform[18]
1. Transparencia	Medianamente fácil de acceder.	Difícil de acceder.	Muy fácil de acceder.
2.Responsabilidades del cliente	• Asegurarse de que el contenido y su uso no infrinjan leyes o políticas. • Obtener los consentimientos requeridos por ley. • Cumplir con las normativas de protección de datos según su rol.		
3. Tipo de obligación	Obligación general de cumplimiento normativo.	Obligación de obtener consentimiento y asumir defensa legal.	Obligación de asegurar cumplimiento según el rol legal y colaboración con el proveedor.
4.Cláusulas de exención o limitación de responsabilidad	Excluyen daños consecuentes, indirectos o especiales, y también lucro cesante o pérdidas económicas intangibles como reputación o clientela. Se excluyen obligaciones de pago y posibles créditos por nivel de servicio.	No lo menciona	Excluyen daños consecuentes, indirectos o especiales, y también lucro cesante o pérdidas económicas intangibles como reputación o clientela.
5. Derechos de propiedad sobre los datos	Propiedad del cliente y responsabilidad del cliente.		
6. Eliminación automática de datos tras finalizar el contrato	No.	Sí, tras 90 días de finalizado el contrato se desactiva la cuenta y se eliminan los datos.	Sí, tras 30 días para recuperación, Google tiene hasta180 días para eliminarlos.
7. Plazo de recuperación después del contrato	Se permite recuperar si el cliente ha pagado. No se establece un plazo específico.	90 días desde la finalización del contrato.	30 días desde la finalización del contrato para solicitar la recuperación.

[16] (CONTRATO DE USUARIO AWS, 2024) (AWS DATA PROCESSING ADDENDUM, 2018)
[17] (Microsoft Privacy Statement, 2025)
[18] (Cloud Data Processing Addendum (Customers), 2025)

Categoría	AWS (Amazon Web Services)[16]	Microsoft Azure[17]	Google Cloud Platform[18]
8. Medidas de seguridad de los datos	Responsabilidad del proveedor que implementa medidas organizacionales, físicas y técnicas. Adicionalmente el cliente puede requerir medidas adicionales como seudonimización o encriptación.	Responsabilidad del proveedor que implementa medidas, técnicas, físicas y organizacionales, incluyendo capacitación de empleados y control de accesos.	Menciona que es una responsabilidad compartida e implementa como proveedor medidas técnicas, físicas y organizacionales; incluye cifrado de información. El cliente debe implementar medidas como backups y llaves de seguridad.
9.Transferencias internacionales de datos	Permite al cliente elegir en qué centro de datos quiere guardar su información y aclara que el cliente será responsable del cumplimiento en relación con la forma en que usted elija utilizar los Servicios o Contenido de AWS, incluyendo la transferencia y el procesamiento de Su Contenido, el suministro de Su Contenido a Usuarios Finales, y la región de AWS en donde ocurra lo anterior.	Se almacenará los Datos del Cliente en reposo dentro de determinadas áreas geográficas importantes (cada una, una Geo área), según lo establecido en los Términos de Productos. Para los servicios de la Unión Europea se almacenarán dentro de la UE.	Dentro de la UE se pueden transferir los datos libremente. Si debe hacerlo fuera de la UE utilizarán las SCC (Cláusulas contractuales estándar) aprobadas por la normativa europea (GDPR). De ser necesario, Google proporcionará al Cliente información relevante sobre Transferencias Restringidas, Controles de Seguridad Adicionales y otras medidas de protección complementarias

3.2.2 Evaluación del riesgo en contratos B2B

En los contratos B2B para servicios en la nube, la evaluación de riesgos debe considerar no solo los aspectos técnicos y operativos, sino también las implicancias jurídicas y normativas derivadas de la externalización del tratamiento de datos.

Uno de los principales riesgos es la **asimetría contractual**, ya que muchos contratos son de adhesión y limitan la responsabilidad del proveedor con cláusulas poco negociables, lo que puede dejar desprotegido al cliente ante fallas del servicio. A ello se suma el **riesgo de incumplimiento normativo**, especialmente si el proveedor no observa adecuadamente las normas, comprometiendo así el cumplimiento del cliente ante los titulares de los datos y las autoridades de control. Otro aspecto crítico es la **falta de trazabilidad y control,** que impide al cliente verificar cómo, dónde y por quién son tratados sus datos, dificultando la rendición de cuentas. La contratación de servicios en la nube implica que la empresa pierde el control y los cuidados de seguridad de los datos. La gestión en la nube puede llevar a que el usuario **pierda el control de la gestión de seguridad**. Surgen conflictos jurídicos debido a la deslocalización de los servicios y la posible aplicación de normativas de varios países.

Otro de los riesgos que una empresa contratante de servicio en la nube debe considerar es la responsabilidad que está tendrá frente al usuario final por ser responsable de tratamiento de datos. Debe considerar que es responsable solidaria en lo que respecta a la seguridad de los datos en la nube lo cual implica riesgos inherentes al sistema como defectos en la programación, inadecuada interoperabilidad con otros sistemas, incompatibilidad de las aplicaciones con la plataforma del sistema operativo. Otros pueden ser externos como introducción de virus y los ataques e intromisiones de hackers.

Por último, en lo que respecta a la empresa proveedora del servicio en la nube se debe considerar la anulación del efecto relativo de los contratos por el orden público de las normas de defensa al consumidor en Argentina.

3.3 Extensión de la responsabilidad entre empresas

3.3.1 Excepción al principio relativo de los contratos.

Este escenario evidencia la necesidad de analizar si existe conexidad contractual entre el proveedor de servicios en la nube y la empresa responsable de tratamiento ante el consumidor, que permita al usuario titular de los datos hacer extensiva la responsabilidad a ambas empresas, como excepción al principio relativo de los contratos.

La conexidad contractual se refiere a un fenómeno jurídico y económico que implica la unión o el enlace de dos o más negocios o contratos. La característica central de la conexidad es que estos contratos, que pueden tener su propia tipicidad y ser

jurídicamente autónomos de forma individual, se encuentran vinculados para lograr una operación económica más amplia o una finalidad económica supra contractual que trasciende el objetivo particular de cada contrato[19].

Las fuentes de la vinculación contractual pueden ser diversas[20]:

- **De fuente contractual (o convencional):** La propia voluntad de las partes enlaza contratos independientes, entrelazando sus efectos. La interpretación de estas cláusulas de conexión debe considerar la operación global concertada.
- **De fuente legal:** Una norma específica reconoce y regula la vinculación. Ejemplos paradigmáticos se encuentran en las leyes de defensa del consumidor (ley 24.240), que priorizan la noción de "relación de consumo" por sobre la de "contrato" y admiten la expansión de efectos a todos los integrantes de la cadena de comercialización, así como en las leyes de tarjeta de créditos (ley 25.065) y leasing (ley 25.248).
- **De fuente fáctica**: Los negocios quedan relacionados en la mera realidad social. En principio, esto no produce efectos jurídicos, salvo que se reconozca un supuesto de conexión o coligación relevante.

Además, la conexión puede clasificarse según diferentes criterios[21]:

- **Genética o Funcional:** Es genética cuando los negocios nacen simultáneamente y vinculados. Es funcional si nacen en diferente tiempo y se vinculan posteriormente durante su ejecución. Esta distinción es relevante para determinar cómo se propagan las vicisitudes.
- **Unilateral o Bilateral/Plurilateral**: Es unilateral cuando el nexo común es una sola de las partes. Es bilateral o plurilateral cuando las partes son idénticas.
- **Interna o Externa:** Es interna la que une negocios mediante alguno de sus elementos y tiene relevancia jurídica. Es externa la mera unión formal en un mismo instrumento

El estudio de la conexidad no solo analiza el vínculo en sí, sino también cómo se propagan los efectos. Esto ha llevado al reconocimiento de una legitimación activa y pasiva ampliada, permitiendo acciones directas y la expansión de responsabilidades (solidarias en algunos casos, como en la ley de defensa del consumidor) hacia otros sujetos del grupo o la red, aunque no hayan contratado directamente con la parte afectada. También implica la expansión de deberes, como el de información y el de custodia, y puede determinar la oponibilidad de ciertas cláusulas.

[19] (Sozzo, 2017)
[20] (Hernández)
[21] (Nicolau)

El nuevo Código Civil y Comercial (CCC) dedica un capítulo a los contratos conexos, reconociendo la finalidad económica común previamente establecida y regulando aspectos como su interpretación, la posibilidad de oponer una exceptio non adimpleti contractus "sistémica", y la expansión de la ineficacia (resolución por frustración de la finalidad supracontractual). Además, en el ámbito del derecho del consumidor, el CCC permite declarar no solo una cláusula sino una "situación jurídica abusiva", lo que guarda relación con la idea de conexidad al evaluar el contexto global de la operación.

3.3.2 Límites legales a la distribución de la responsabilidad.

La relación contractual entre el responsable de tratamiento y el encargado de tratamiento, según la clasificación antedicha, es de fuente fáctica y de carácter funcional, porque, aunque los contratos pueden no nacer al mismo tiempo, se vinculan durante su ejecución para cumplir con una finalidad económica común: el tratamiento y almacenamiento de datos personales para brindar servicios al usuario final.

En ciertos casos, es posible extender esa responsabilidad, aunque no exista contrato directo entre el proveedor de nube y el usuario final. Esto puede darse por:

- La conexidad contractual funcional y la finalidad económica común (art. 1073 del Código Civil y Comercial): si los contratos están orientados a lograr una finalidad supra contractual conjunta (por ejemplo, garantizar la seguridad y disponibilidad del servicio al usuario), puede propagarse la ineficacia o incluso la responsabilidad.
- Aplicación analógica de normas de defensa del consumidor (cuando corresponde): aunque estemos en el plano B2B, si la empresa contratante actúa como intermediaria en una cadena que termina afectando a un consumidor, la jurisprudencia podría extender la responsabilidad solidaria (como ocurre en relaciones de consumo por el art. 40 de la Ley 24.240).
- Deberes amplificados: como el deber de información y de custodia, que pueden extenderse al proveedor de servicios si se considera parte del sistema que posibilita el servicio final al usuario.

Las cláusulas que limitan la responsabilidad del proveedor de servicios en la nube son típicas y válidas en los contratos B2B, pero tienen su límite en el orden público. No pueden exonerar responsabilidad por dolo, culpa grave o violación de normas de orden público (como la Ley de Protección de Datos Personales o la LDC si aplica); son interpretadas restrictivamente cuando hay asimetrías entre las partes, desequilibrio de poder o si afectan derechos fundamentales (como el derecho a la protección de datos personales) y; pueden ser inoponibles al usuario final si se reconoce conexidad contractual o si afectan el núcleo de la obligación hacia el consumidor.

3.3.3 Responsabilidad solidaria en cadenas contractuales tecnológicas.

En resumen, la conexidad contractual es un concepto fundamental para comprender las relaciones negociales modernas, especialmente en la contratación masiva y en redes empresariales, que permite analizar conjuntos de contratos como una unidad funcional dirigida a un fin económico común, flexibilizando el principio clásico de la relatividad contractual para atribuir efectos más allá de las partes directas de cada negocio individual.

Un ejemplo de esta extensión y el límite al efecto relativo de los contratos entre empresas es el caso Cambridge Analytica. La filtración de datos de millones de usuarios de Facebook y su posterior utilización con fines políticos puso en evidencia los riesgos asociados a la gestión de datos en plataformas digitales. La posterior quiebra y disolución de Cambridge Analytica evidencia cómo la responsabilidad en la gestión de datos personales puede proyectarse más allá del responsable primario del tratamiento —en este caso, Facebook— alcanzando también a terceros intervinientes en la cadena negocial. La incapacidad de Cambridge Analytica para soportar el impacto reputacional y jurídico derivado del uso indebido de datos pone de manifiesto que, las consecuencias pueden extenderse solidariamente, por el orden público y la calidad de los derechos en juego, más allá de la configuración del vínculo y la estructura de obligaciones asumidas. Esta dinámica se presenta con particular claridad en los modelos de negocio vinculados a contratos tecnológicos, donde intervienen múltiples actores coordinados para alcanzar una finalidad económica común y cuya operativa suele involucrar el tratamiento de datos personales como insumo central.

4. Propuestas y consideraciones finales

4.1 Necesidad de mayor precisión contractual en la asignación de riesgos.

En los servicios de cloud computing, la precisión en la asignación de riesgos contractuales se vuelve crucial para garantizar seguridad jurídica. Como se observa en los contratos tipo analizados de los principales proveedores de servicios en la nube, muchas veces las cláusulas son generales, limitativas o redactadas unilateralmente, lo que deja al cliente en una posición de vulnerabilidad frente a fallos o incumplimientos. Esta imprecisión se acentúa en relaciones B2B donde la empresa contratante, en su rol de responsable de tratamiento, asume frente al usuario final deberes que no siempre logra trasladar adecuadamente al proveedor. La falta de cláusulas claras sobre seguridad, subcontrataciones, notificación de incidentes o mecanismos de control compromete el cumplimiento normativo y dificulta la atribución de responsabilidades.

Por ello, resulta imprescindible avanzar hacia contratos que reflejen con mayor detalle los riesgos previsibles, el reparto efectivo de obligaciones y las consecuencias jurídicas

de los incumplimientos, a fin de evitar zonas grises que expongan a las partes y, en última instancia, a los derechos de los titulares de los datos.

4.2 Propuesta de buenas prácticas para empresas que contraten servicios en la nube.

A partir del análisis realizado, puede observarse que las relaciones contractuales entre empresas en el ámbito de los servicios en la nube presentan una asimetría significativa, especialmente cuando las empresas contratantes —frecuentemente pymes o entidades sin gran poder de negociación— deben adherirse a contratos prediseñados por grandes proveedores tecnológicos. Esta situación requiere que los responsables del tratamiento de datos adopten un enfoque preventivo, estratégico y transversal.

En ese sentido, se propone el siguiente conjunto de buenas prácticas, con el fin de reducir los riesgos jurídicos, aumentar la trazabilidad del tratamiento de datos y fortalecer una cultura organizacional orientada al cumplimiento normativo:

- **Evaluación previa del proveedor**: antes de contratar, la empresa debe realizar una auditoría del proveedor en base a sus certificaciones (ISO/IEC 27001, 27018, entre otras), estándares internacionales y antecedentes en materia de privacidad. Esto no solo permite elegir con mayor criterio, sino también sustentar decisiones ante eventuales litigios.
- **Negociación o revisión crítica del contrato tipo**: aun en casos de contratos de adhesión, se recomienda negociar o solicitar cláusulas complementarias sobre:
    - Subencargados del tratamiento.
    - Medidas de seguridad específicas.
    - Notificación de incidentes.
    - Cooperación activa con el responsable.
- **Capacitación interna en compliance de privacidad**: todos los integrantes de la organización, sin importar jerarquía o sector, deben recibir formación periódica sobre la importancia de la protección de datos personales y sus implicancias legales. Esto incluye a sectores técnicos, administrativos, comerciales o de atención al cliente, ya que todos manejan —directa o indirectamente— datos de usuarios finales. La capacitación en compliance permite detectar riesgos, fomentar una cultura de responsabilidad y asegurar que las buenas prácticas se traduzcan en la operativa diaria.
- **Supervisión continua y trazabilidad**: implementar mecanismos de control interno como registros de actividades, revisiones periódicas, controles de acceso, auditorías y simulacros ante incidentes. Esta trazabilidad permite demostrar cumplimiento y adoptar medidas correctivas a tiempo.
- **Mecanismos contractuales de verificación externa**: pactar, en lo posible, el derecho a auditar o al menos recibir informes técnicos del proveedor y sus

subcontratistas, como forma de supervisar el cumplimiento de sus obligaciones contractuales.

Estas prácticas son escalables y adaptables al tamaño y capacidad de cada empresa. No obstante, su adopción representa un avance sustancial en materia de responsabilidad proactiva, cumplimiento normativo y resguardo de los derechos de los titulares de datos.

4.3 Reflexión final sobre la importancia de proteger los derechos fundamentales en las relaciones entre empresas tecnológicas.

Las relaciones contractuales entre empresas no pueden desentenderse del marco de protección de los derechos fundamentales, en particular el derecho a la privacidad y a la protección de datos personales. Si bien las contrataciones B2B suelen centrarse en eficiencias operativas y reducción de costos, lo cierto es que muchas de estas relaciones tienen como objeto, directa o indirectamente, el tratamiento de información de personas físicas.

El caso Cambridge Analytica revela con claridad cómo decisiones tomadas dentro de una cadena empresarial pueden tener impactos directos sobre derechos individuales, aun cuando no exista un vínculo contractual entre el titular y todos los actores intervinientes. En este sentido, el reconocimiento de la conexidad contractual y la posibilidad de extender efectos y responsabilidades más allá de las partes firmantes reflejan una evolución del derecho hacia una mirada más sistémica y protectora.

Proteger los derechos fundamentales implica no solo cumplir con normas específicas, sino también asumir un compromiso ético con el respeto a la dignidad humana en el diseño y ejecución de modelos de negocio basados en datos.

5. Conclusión

El presente trabajo ha puesto de manifiesto los múltiples desafíos jurídicos que surgen en las relaciones B2B en el entorno de los servicios en la nube, especialmente cuando estas involucran el tratamiento de datos personales. La transformación digital y el uso extendido de tecnologías cloud han modificado la forma en que las empresas operan, obligando al derecho a repensar sus categorías tradicionales y a adoptar un enfoque más sistémico e integrador.

En este contexto, el análisis del fenómeno de la conexidad contractual permite comprender cómo múltiples contratos —formalmente autónomos— pueden estar funcionalmente vinculados, generando una extensión de la responsabilidad entre empresas que intervienen en una misma operación económica. Esta extensión no se limita al plano doctrinario, sino que encuentra respaldo en normas de orden público,

como las leyes de protección de datos y de defensa del consumidor, que priorizan la tutela efectiva de los derechos fundamentales.

La figura del responsable del tratamiento de datos ya no puede considerarse como único sujeto obligado: los proveedores de servicios, subencargados, aliados tecnológicos y demás actores que intervienen en la cadena contractual comparten —de manera más o menos explícita— deberes de diligencia, seguridad y colaboración. Por ello, el diseño de contratos más precisos, la implementación de buenas prácticas empresariales y la capacitación continua del personal resultan elementos claves para cumplir no solo con la letra de la ley, sino también con su espíritu.

En definitiva, el derecho a la protección de los datos personales impone a las empresas un deber ético y jurídico colectivo, que trasciende fronteras jurídicas formales y obliga a actuar con transparencia, proporcionalidad y responsabilidad. Solo una visión integradora que combine innovación tecnológica con principios de legalidad y derechos humanos podrá garantizar que el desarrollo empresarial no se realice a costa de la dignidad informacional de las personas.

Bibliografía

Abdelnabe Vila, M. C.-C. (2020). Perspectivas de la Protección de Datos Personales: status quo y proyeccione. *La Ley*.

Agencia de acceso a la Información Pública. (Junio de 2023). Proyecto de LEY DE PROTECCIÓN DE LOS DATOS PERSONALES. *Mensaje 87/2023*. Obtenido de https://www.argentina.gob.ar/sites/default/files/mensajeyproyecto_leypdp2023.pdf

Aller, C. F. (2012). Algunos retos de la protección de datos en la sociedad del conocimiento Especial detenimiento en la computación en la nube. *Revista de Derecho UNED Nº.10*.

AWS DATA PROCESSING ADDENDUM. (2018 de Mayo de 2018). Obtenido de https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf

BBC News Mundo. (2019). *Cambridge Analytica: la multa récord que deberá pagar Facebook por la forma en que manejó los datos de 87 millones de usuarios*. Obtenido de https://www.bbc.com/mundo/noticias-49093124

Cloud Data Processing Addendum (Customers). (2025). Obtenido de https://cloud.google.com/terms/data-processing-addendum?hl=es_419

Compagnucci, M. C. (Junio de 2022). *Derecho y Economía en la Nube y Big Data: Un modelo contractual más eficiente para reasignar la*. Obtenido de Research Gate: https://www.researchgate.net/publication/361530789_Derecho_y_Economia_en_la_Nube_y_Big_Data_Un_modelo_contractual_mas_eficiente_para_reasignar_la_propiedad_de_los_datos

CONTRATO DE USUARIO AWS. (17 de Mayo de 2024). Obtenido de https://d1.awsstatic.com/legal/aws-customer-agreement/AWS_Customer_Agreement_2024-05-17_ES(LA).pdf

Diccionario de la lengua española. (17 de 4 de 2025). Obtenido de https://dle.rae.es/dato

El Senado y Cámara de Diputados de la Nación Argentina. (1994). *InfoLeg*. Obtenido de https://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm

Estella, F. D. (2024). *El sector cloud ante el Derecho de la Competencia: el próximo reto*. Obtenido de Dialnet: https://dialnet.unirioja.es/servlet/articulo?codigo=9611955

Halabi, Ernesto c/ P.E.N. – ley 25.783 – dto. 1563/04 s/ amparo ley 16.986, Fallos: 331:2784 (CSJN 2008).

Han, B.-C. (2013). *La Sociedad de la Transparencia*.

Hernández, C. A. (s.f.). ACERCA DEL PRINCIPIO DE RELATIVIDAD DE LOS EFECTOS DEL CONTRATO.

Ley 25.326. (4 de Octubre de 2000). *INFOLEG*. Obtenido de PROTECCION DE LOS DATOS PERSONALES.

Ley 26.994 Codigo Civil y Comercial de la Nación. (2014). Obtenido de https://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/235975/texact.htm

Marzo, J. V. (2018). LA PRIVACIDAD EN EL ENTORNO DEL CLOUD COMPUTING. España: REUS. Obtenido de https://dialnet.unirioja.es/servlet/libro?codigo=726494

Microsoft Privacy Statement. (Marzo de 2025). Obtenido de https://azure.microsoft.com/en-us/explore/trusted-cloud/privacy

Nicolau, N. L. (s.f.). Los negocios jurídicos conexos. *Centro de Investigaciones de Derecho Civil de la Facultad de Derecho de la Universidad Nacional de Rosario*.

Organización de los Estados Americanos. (22 de Noviembre de 1969). Convención Americana sobre Derechos Humanos "Pacto de San José de Costa Rica". Obtenido de https://www.oas.org/dil/esp/1969_Convenci%C3%B3n_Americana_sobre_Derechos_Humanos.pdf

Petersen, J. C. (2024). *Comparación de las Principales Plataformas en la Nube: AWS vs. Azure vs.Google Cloud*. Obtenido de LinkedIn: https://www.linkedin.com/pulse/comparaci%C3%B3n-de-las-principales-plataformas-en-la-nube-juan-carlos-glowf?originalSubdomain=es

Red Iberoamericana de Protección de Datos. (Abril de 2021). Recomendaciones para le Tratamiento de Datos Personales mediante Servicios de Computación en la Nube. Obtenido de https://www.redipd.org/sites/default/files/2021-06/recomendaciones-tratamiento-datos-personales-servicios-nube.pdf

Sozzo, G. (2017). LAS FUNCIONES DE LA CONEXIDAD CONTRACTUAL EN EL DERECHO DEL CONSUMIDOR: ARGUMENTO COADYUVANTE Y EFECTOS PROPIOS. En J. M. Iturraspe, *Contratos*.

Unión Europea. (4 de Mayo de 2016). *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 (Reglamento General de Pro*. Obtenido de Diario Oficial de la Unión Europea (DOUE).