Consideraciones legales sobre datos personales en fusiones y adquisiciones

Legal considerations on personal data in mergers and acquisitions

— Lisandro Frene* y Juan Aberg Cobo** —

Resumen

En los últimos quince años, las nuevas tecnologías –'alimentadas' en base al procesamiento masivo de datos –crecieron a un ritmo tan vertiginoso que abarcaron prácticamente toda la sociedad, las industrias y actividades mercantiles. Esta expansión tecnológica sin precedentes –de la cual los datos son su combustible– generó legislación específica sobre tratamiento de datos personales. Así es que, actualmente, en las transacciones de fusiones y adquisiciones (M&A) el análisis jurídico de cuestiones de *data privacy* de la empresa *target* resulta algo corriente y hasta imprescindible en cualquier *due diligence* y operación mínimamente seria. En este artículo procuraremos reseñar las principales consideraciones jurídicas insoslayables sobre datos personales a tener en cuenta en las operaciones de fusión y/o adquisición, en las respectivas etapas *pre* y *post-closing* de dichas transacciones.

Palabras clave

Datos personales, transacción, *due diligence*, contingencias obligaciones.

Abstract

In the last fifteen years, new technologies –'fueled' by massive data processing– have grown at such a vertiginous pace that they have encompassed virtually all society, industries and business activities. This unprecedented technological expansion –of which data is its fuel– generated specific legislation on the processing of personal data. Thus, nowadays, in mergers and acquisitions (M&A) transactions, the legal analysis of data privacy issues of the target company is commonplace and even essential in any due diligence and minimally serious operation. In this article we will try to outline the main unavoidable legal considerations on personal data to be considered in merger and/or acquisition operations, in the respective pre and post-closing stages of such transactions.

Keywords

Personal data, transaction, due diligence, contingencies, contracts.

* Abogado por la Universidad de Buenos Aires. LLM en la Yeshiva University de Nueva York (2001). Socio encargado del área de IT & Data Privacy del Estudio Richards, Cardinal, Tützer, Zabala, Zaefferer SC. Cybersecurity Officer y miembro del Technology committee de la International Bar Association. Correo: frene@rctzz.com.ar

** Abogado por la Universidad Católica Argentina. Cursó el Programa de Derecho y Tecnología de la Universidad de San Andrés y el Curso Internacional de Datos Personales en la misma Universidad (2022). Miembro del área de IT & Data Privacy del Estudio Richards, Cardinal, Tützer, Zabala, Zaefferer SC. Correo: aberg@rctzz.com.ar

1. Introducción

Las cuestiones sobre bases de datos eran un ítem prácticamente inexistente entre las consideraciones legales a analizar previo a realizar una transacción de fusión o adquisición societaria. Ello era natural, por así decirlo, salvo por puntuales excepciones, pues casi no existía legislación ni conflictos al respecto. En los últimos quince años, particularmente desde el advenimiento de la llamada cuarta Revolución Industrial, las nuevas tecnologías –'alimentadas' en base al procesamiento masivo de datos– crecieron a un ritmo tan vertiginoso que abarcaron prácticamente toda la sociedad, las industrias y actividades mercantiles. Hoy, siete de las diez compañías más valiosas del mundo son tecnológicas; y las que no lo son, dependen decisivamente de la tecnología para producir, distribuir y/o comercializar sus bienes y/o servicios, cualquiera sea el rubro en que se desempeñen. Esta expansión tecnológica sin precedentes –de la cual los datos son su combustible– generó legislación específica sobre tratamiento de datos personales. En 2001, escasos países contaban con este tipo de normativa, siendo Argentina el único en América. Hoy, más de 130 países (y la mayoría de Sudamérica[1]) cuentan con normativa sobre datos personales: ello, dado que los datos tienen un valor, representa un activo fundamental (muchas veces el principal activo) de una compañía. El modo en que los datos pueden ser tratados –entendido en el sentido amplio que la legislación comparada le atribuye a este último término– adquiere consecuencias jurídicas muy concretas: de allí el surgimiento de su regulación, que continúa *in crescendo*.

Así es que, actualmente, en las transacciones el fusiones y adquisiciones (M&A), el análisis jurídico de cuestiones de *data privacy* de la empresa *target* resulta algo corriente y hasta imprescindible en cualquier *due diligence* y operación mínimamente seria. Desde cuestiones registrales, hasta incidentes de ciberseguridad (por ejemplo, individualización de ellos, medidas contingentes tomadas, etc.), origen y categorización de los datos, pasando por cumplimientos normativos, cláusulas de *data privacy* en contratos con terceros, transferencia internacional de datos, pedidos de habeas data y/o sanciones y/o auditorías al respecto, por citar solo un par de títulos. Se trata de un análisis necesariamente transversal que debe realizarse cualquiera sea el sector de la industria involucrado en este tipo de transacciones y que generalmente debe complementarse con otras áreas del derecho (laboral, societario, bancario, etc.) pues todas ellas se ven impactadas por la normativa de datos personales.

En este artículo procuraremos reseñar las principales consideraciones jurídicas sobre datos personales a tener en cuenta en las operaciones de fusión y/o adquisición. Lógicamente, variarán según las particularidades específicas y la estructura de la transacción bajo análisis (por ejemplo, fusión, compraventa accionaria, adquisición de una unidad de negocios o fondo de comercio, etc.). En cualquier caso, el objetivo es reseñar someramente los institutos conceptuales de *data privacy* insoslayables en las etapas *pre* y *post-closing*, así como las cláusulas que –a grandes rasgos– deberían incluirse en los documentos que instrumenten este tipo de transacciones.

---

1 Dentro de estos países se encuentran: Argentina (PROTECCION DE LOS DATOS (infoleg.gob.ar)),Brasil (http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm), Chile (Ley Chile - Ley 19628 - Biblioteca del Congreso Nacional (bcn.cl)), Colombia (LEY 1581 DE 2012 (suin-juriscol.gov.co)), Ecuador (1162059_-_LEY_ORGÁNICA_DE_PROTECCIÓN_DE_DATOS_PERS_202107011248165227 (www.gob.ec)), Perú (LEY DE PROTECCIÓN DE DATOS PERSONALES.indd (www.gob.pe)), Uruguay (Ley N° 18331 (impo.com.uy)). En el caso de Bolivia y Paraguay, las disposiciones sobre protección de datos personales no se encuentran, a la fecha, centralizadas en una ley genérica, sino en distintas normativas. En el caso boliviano, la protección de datos personales es legislada en la Constitución Política de Bolivia en sus arts. 21, 130 y 131 (CONSTITUCION.pdf (gacetaoficialdebolivia.gob.bo)), el Código Procesal Constitucional (Código Procesal Constitucional – Protección de datos personales Bolivia (protecciondedatos.bolivia.bo)), Decreto Supremo N°1793, reglamentario de la Ley N°164 (DS-N°-1793-Reglamento-a-la-Ley-N°164-para-el-Desarrollo-de-Tecnologías-de-la-Información-y-Comunicación.pdf (ctic.gob.bo)) y la Ley de Ciudadanía Digital N°1080 del año 2018, en su art. 12 (Ley-1080-Ciudadanía-Digital..pdf). En el caso de Paraguay, la protección de datos personales se encuentra legislada en la Constitución de la República en sus arts. 33, 36, 45, 135 (Constitución de la República de Paraguay, 1992 (oas.org)), Ley 6354/2020 de Protección de Datos Personales Crediticios (LEY+6534.pdf (bacn.gov.py)), Ley 4868/2013 de Comercio Electrónico (20140409095515.pdf (bacn.gov.py)), Ley 4017/2010 de Validez Jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico, en su art. 34 (20150709092101.pdf (bacn.gov.py)), Ley 5282/2014 (https://www.bacn.gov.py/leyes-paraguayas/3013/libre-acceso-ciudadano-a-la-informacion-publica-y-transparencia-gubernamental). Por fuera del ámbito de Sudamérica, se encuentran, por ejemplo: México (en el sector privado, regulado por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (diputados.gob.mx y en el sector público regulado por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (diputados.gob.mx)), Panamá (Gaceta Oficial Digital (antai.gob.pa) y su reglamento Gaceta Oficial Digital (antai.gob.pa)), Canadá (cuenta con dos leyes federales de aplicación, la 'Privacy Act' (Privacy Act (justice.gc.ca)) y la 'Personal Information Protection and Electronic Documents Act' (Personal Information Protection and Electronic Documents Act (justice.gc.ca)), Costa Rica (Microsoft Word - leydeprotecciondelapersona (tse.go.cr)), El Salvador con la Ley de Acceso a la Información Pública (www.transparencia.gob.sv/institutions/iaip/documents/302297/download), Nicaragua con la Ley de Protección de Datos Personales (LEY DE PROTECCIÓN DE DATOS PERSONALES (asamblea.gob.ni)), República Dominicana con la Ley 172/2013 (Ley No. 172-13 Protección de los Datos (sb.gob.do))y Cuba con la Ley 149/2022 (goc-2022-o90_0.pdf (gob.cu)). Las citas a las leyes de *data privacy* distintas a la Argentina son meramente de carácter referencial.

2. Inicio de las negociaciones: previsiones para el intercambio de información.

Independientemente del tipo y forma de la potencial transacción, usualmente al comenzar las negociaciones, las partes suscriben un documento mediante el cual expresan su intención de iniciar tratativas sobre intercambio de información con el fin de, en caso de llegar a un acuerdo, firmar los documentos que reflejen la transacción final. En este documento inicial (típicamente una carta de intención, memorándum de entendimiento o similar) suelen incluirse compromisos 'no vinculantes' (se denominan así por estar condicionados a que las partes acuerden los aspectos definitivos de la negociación iniciada) y cláusulas obligatorias. Entre estas últimas es común incluir cláusulas de no exclusividad; no competencia por un plazo determinado; cláusulas de no captación de empleados, jurisdicción y ley aplicable; y, casi siempre, cláusulas de confidencialidad. Dentro de este tipo de cláusulas vinculantes, deberán incluirse cláusulas sobre el tratamiento de los datos que las partes habrán de intercambiarse y las obligaciones de cada una de ellas al respecto, en concordancia con la legislación de datos personales en las jurisdicciones involucradas, ya sea que se concluya o no el negocio inicialmente propuesto.

Las partes de la negociación comenzarán a intercambiarse información tendiente a concluir la misma: en general, la vendedora proveerá a la potencial compradora información de la empresa a ser adquirida, típicamente resumida en un *due diligence checklist*. Gran parte de esa información estará constituida por "datos personales" (conforme las definiciones de las leyes aplicables en la materia). En este punto, cabe recordar que las empresas pueden ser "responsables" (*controllers*) de esas bases de datos, pero los titulares de tales datos son las personas físicas a las que se refiere esa información; y esos titulares probablemente no hayan dado su consentimiento y probablemente ignorarán este intercambio de sus datos entre las empresas de la transacción.

Entonces, en esa carta de intención inicial, además de la típica cláusula de confidencialidad, deberán incluirse cláusulas vinculantes para la parte receptora de la información respecto de las medidas de seguridad que adoptará para salvaguardar los datos personales recibidos; la finalidad –acotada– que le dará a tales datos; las restricciones de acceso para dichos datos, circunscriptas únicamente a quienes intervengan en el *due diligence* y solo con ese propósito; los contratos o cláusulas que habrá de incluir en los contratos con sus subcontratistas o proveedores intervinientes en la transacción que accedan a tales datos; el curso de acción a seguir en caso de recibir un pedido de acceso por parte de los titulares de los datos; el tiempo durante el cual los mantendrá; y el modo y compromiso de destruir tales datos en caso de que no se concrete la transacción, así como la constancia de que tal destrucción se ha llevado a cabo y la inexistencia de copias de tales datos; y los distintos supuestos de responsabilidad en caso de un incidente de seguridad de tales datos, fuga o acceso indebido a los mismos, previéndose las consecuencias para tales supuestos.

Corresponde tener presente que, en esta etapa precontractual y como principio general, si la transacción no se concluye por falta de acuerdo entre las partes respecto de los elementos esenciales de la misma (precio, plazo, bienes a adquirir, forma de pago, u otros aspectos) no habrá responsabilidad de las partes al respecto. No obstante, desde el momento mismo que existe transferencia de datos personales de una parte a la otra, sí puede haber responsabilidad de las partes (incluso solidaria de ambas partes frente al titular del dato) por tratamiento indebido de los mismos y esto conviene preverlo adecuadamente en el instrumento que da inicio a la negociación.

3. Auditoría *(due diligence)* de la sociedad a adquirir: aspectos de datos personales a relevar.

Luego de instrumentarse formalmente el inicio de las negociaciones, habitualmente, comienza la auditoría de la sociedad *target*, comúnmente conocida como *due diligence*. En dicho proceso, la parte potencialmente vendedora pone a disposición de la potencial compradora la información y documentación legal y contable de dicha sociedad –que lógicamente implica revelarle datos personales– para que esta última evalúe el status de la misma, sus contingencias y, en función de ello, el valor y los términos de la pretendida adquisición. Desde el punto de vista jurídico, el listado de información a relevar suele condensarse en un listado (*due diligence checklist*) segmentado según las distintas áreas del derecho (laboral, contencioso, administrativo, societario, ambiental, etc.). Como decíamos al inicio, en la última década se ha agregado a ese *checklist* el área de datos personales como un área en sí misma que, paradójicamente, resulta transversal a todas las demás en el sentido que impacta en todas ellas, ya que todas implican el tratamiento de datos personales.

A continuación, detallaremos algunos aspectos sobre *data privacy* que entendemos deberían incluirse a la hora de confeccionar el *checklist* y considerarse al implementar el *due diligence* sobre el *target* encomendado. La presente enumeración es genérica y enunciativa, pudiendo la misma modificarse o ampliarse tomado en cuenta factores particulares de las empresas involucradas en la potencial transacción.

3.a Inscripción en registros de bases de datos

Es habitual en varias legislaciones sobre datos personales la imposición del deber legal de inscribirse en algún tipo de "registro de bases de datos" o denominación similar, administrado por la autoridad de aplicación de la ley de datos personales de la jurisdicción en cuestión[2]. El incumplimiento de esta obligación registral suele generar sanciones de distinto tipo.

Tal es el caso, por ejemplo, de Argentina, en donde la Ley N°25.326 de Protección de Datos Personales (en adelante, "LPDP Argentina") expresamente prevé en su artículo 21 que "todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes debe inscribirse en el Registro que al efecto habilite el organismo de control" (Congreso de la Nación Argentina, 2000, p. 7) junto con los requisitos que deben cumplir. La falta de inscripción deja expuesta a la empresa infractora a las sanciones pertinentes[3]. Criterio similar observamos en Perú, dado que la Ley de Protección de Datos Personales de dicho país (en adelante, "Ley de Perú"[4]) impone la obligación de inscribir en el Registro Nacional de Protección de Datos Personales, "los bancos de datos personales de administración pública o privada, así como los datos relativos a estos que sean necesarios para el ejercicio de los derechos que corresponden a los titulares de datos personales" (Congreso de la República del Perú, 2011, p. 6). En caso de realizar tratamiento de datos sin haber inscrito las correspondientes bases de datos en el antedicho Registro Nacional de Protección de Datos Personales, ello será considerado como una infracción "grave" según la Ley de Perú (Congreso de la República del Perú, 2011, p. 6), quedando expuesto el *target* a las sanciones pertinentes[5].

En función de ello, es relevante verificar si la sociedad que se está pretendiendo adquirir ha cumplido en debida forma con esta obligación registral formal. En el caso de Argentina, la verificación puede realizarse mediante una consulta en el Registro Nacional de Bases de Datos Personales, de forma gratuita[6]; en Perú, el procedimiento es similar al argentino. Conforme señala Jessica Hondermann[7], "la labor de verificación es relativamente sencilla pues el Registro de Protección de Datos Personales[8] es público y puede ser revisado de forma gratuita" (comunicación personal, 30 de octubre de 2023).

3.b Políticas de privacidad

Las políticas de privacidad de una empresa son cada vez más usuales –cualquiera sea el tamaño de la empresa– e incluso un requisito regulatorio en varias jurisdicciones[9]. Sus términos tienen consecuencias y contingencias cada vez más concretas, extendiéndose desde la relación con consumidores y clientes hasta los deberes de los empleados de la empresa en el trato con la información que ma-

2 Si bien esta obligación se encuentra tanto en Argentina y en Perú como adelantaremos a continuación, en el plano europeo, el Reglamento General de Protección de Datos (en adelante, "GDPR") no la incorpora. Sin embargo, el art. 30 del GDPR prevé una obligación similar, dado que impone a los *controllers* y a *processors* (y sus respectivos representantes) llevar adelante la confección de un registro interno – el cual puede ser puesto a disposición de la autoridad de aplicación- en donde detallen determinadas cuestiones del tratamiento.

3 No inscribir las bases de datos en el registro pertinente es considerado una "infracción leve" por la Resolución 240/2022 AAIP. No obstante, ello, en caso de no inscribirlas luego de un requerimiento por la autoridad de aplicación, constituirá un agravante, incrementándose de dicha manera las sanciones a aplicar por dicho incumplimiento.

4 Ley de Protección de Datos Personales del Perú N°29.733.

5 Según el artículo 39 inciso 2 de la Ley de Perú, las infracciones graves serán sancionadas con multa de más de 5 Unidades Impositivas Tributarias (UIT) hasta 50 UIT. A la fecha de redacción del presente, una UIT equivale a S/4950 (USD 1296,25).

6 Buscador del Registro Nacional de Bases de Datos Personales | Argentina.gob.ar

7 Jessica Hondermann Gómez es abogada experta en el derecho protección de datos personales en Perú, miembro del Estudio Martinot Abogados. Agradecemos la colaboración de la Dra. Hondermann Gómez para la redacción del presente artículo.

8 https://prodpe.minjus.gob.pe/prodpe_web/BancoDato_verResultado.

9 Art. 24 GDPR. En el caso de Argentina, si bien no existe una norma que obligatoriamente establezca el deber de contar con una política de privacidad, la AAIP (autoridad de aplicación de la LPDP Argentina) sí lo considera como tal. Ello en base a los principios del art. 4 LPDP Argentina y a la Disposición AAIP 18/2015 sobre "Guía De Buenas Prácticas En Privacidad Para El Desarrollo De Aplicaciones". Esta última norma dispone en su Anexo I que el establecimiento de una política de privacidad constituye "[u]no de los pasos más importantes para respetar la privacidad de los titulares de datos, es desarrollar una Política de Privacidad que

nejan y/o a la que tienen acceso. El alcance de los derechos y obligaciones de una empresa respecto de los datos que maneja en gran medida dependerá de la existencia o no de este tipo de políticas y de cómo han sido comunicadas a sus destinatarios. Por eso será conveniente en el *due diligence* constatar la existencia o no de políticas de privacidad (es habitual, por ejemplo, que exista una política de privacidad para proveedores, otra para clientes y otra distinta para empleados), el modo de comunicación de la misma, el alcance de sus términos y el grado de cumplimiento de lo establecido en dicha política.

3.c Consentimiento de los titulares de los datos y otras bases para el tratamiento

¿De qué modo la empresa llegó a hacerse de los datos personales que maneja? ¿Obtuvo el consentimiento del titular de los datos o los recolectó en base a otros supuestos legales que la habilitan a este fin? ¿Está ello documentado? ¿Tiene sustento legal?

Al realizar la auditoría de la empresa a adquirir, debemos considerar que el tratamiento de datos personales será lícito en tanto y en cuanto las partes involucradas en el mismo lo realicen basándose en un principio permitido por ley y los datos personales tratados sean solamente utilizados con la finalidad que motivó su recolección[10]. Como principio general, los datos pueden ser tratados con previo consentimiento escrito e informado de su titular a tal efecto, pero existen en las legislaciones de la materia diversas excepciones a este principio general que habilitan la validez legal de su tratamiento[11].

De allí surge la trascendencia de corroborar si la empresa a adquirir efectuó –y efectúa– su tratamiento de datos de acuerdo a los principios de licitud del mismo, como también si el mismo se ajusta a las finalidades que habilitaron dicho tratamiento. El incumplimiento de las bases legales para el tratamiento puede derivar en procedimientos de oficio o en reclamos de los titulares de los datos y/o en la imposición de sanciones de diferente cuantía hacia el infractor por parte de la autoridad de aplicación[12], contingencias que, en caso de producirse, deberán ser asumidas –en todo o en parte– por el comprador de la empresa adquirida. Es por ello que, conforme señala Jessica Hondermann, "se sugiere solicitar muestras aleatorias de los formatos de consentimientos (autorizaciones escritas, políticas de privacidad, carteles informativos, glosas, etc.) que el target emplee para cada uno de sus bancos de datos" (comunicación personal, 30 de octubre de 2023).

3.d Medidas de seguridad de datos personales

Otro de los aspectos centrales de *data privacy* es aquel vinculado a la seguridad de los datos y a las medidas organizativas técnicas y administrativas que el responsable de la base de datos (en este caso, la empresa a adquirir) debe tomar para garantizar –valga la redundancia– la seguridad e integridad de los datos personales objeto del tratamiento.

Este aspecto es receptado por las legislaciones en materia de *data privacy*, aunque de manera dispar, dado que existen legislaciones que imponen el de-

explique claramente qué tipo de información se recaba, cómo se usa y con quién la compartes" (Dirección Nacional de Protección de Datos Personales, 2015), a la vez que menciona varios parámetros que la misma debe cumplir. También existen otras normas de dicho organismo que indirectamente mencionan la obligatoriedad de las políticas de privacidad, como la Disposición AAIP 3/2012 que establece la facultad de la AAIP de inspeccionar a las empresas y requerirles su Política de Privacidad para evaluar el tratamiento de datos que realizan. En el caso de Perú, el art. 18 de la Ley de Perú expresamente trata las políticas de privacidad como un mecanismo para satisfacer el derecho de información de los titulares del dato.

10 Este principio se trata de un principio elemental de *data privacy*. A modo de ejemplo, el GDPR en su art. 5 inciso "b" prohíbe expresamente el tratamiento de datos personales de manera incompatible con las finalidades que motivaron la recolección. En el plano de Latinoamérica, la LPDP Argentina en su art. 4 inciso 3 y la Ley de Perú en su artículo 6 consagran este principio expresamente.

11 Art. 6 GDPR. Art. 5 inciso 2 "d" LPDP Argentina. Art. 14 Ley de Perú.

12 En el plano europeo, en base al art. 83 del GDPR *in fine*, estipula que el infractor a las disposiciones del consentimiento puede ser sancionado con multas de hasta €20.000.000 o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía. En el caso de Argentina, según la Resolución AAIP 240/2022, tratar los datos personales sin contar con una base de legitimación adecuada será considerado como una infracción 'grave' y como infracción 'muy grave' el tratamiento de datos personales en forma ilegítima o con menosprecio de los principios y garantías establecidos en la LPDP Argentina y normas reglamentarias. Para el caso de las infracciones graves, si bien los montos por cada infracción no son superiores a AR$ 90.000 y en el caso de infracciones muy graves, los montos no son superiores a AR$100.000, la Resolución AAIP 244/2022 indica que cuando un acto administrativo condenatorio incluya más de una sanción pecuniaria por idéntica conducta sancionable dentro de los niveles establecidos en la Resolución AAIP 240/2022, el tope máximo será de AR$ 10.000.000 para las infracciones graves y de AR$15.000.000 para las infracciones muy graves. En el caso de Perú, el art. 38 de la Ley de Perú indica que tratar datos personales sin consentimiento del titular será considerado una infracción 'leve', pudiendo ser sancionado el infractor con multas cuyo rango varía entre 0.5 y 5 Unidades Tributarias conforme el art. 39 de la Ley de Perú (a la fecha de redacción del presente, entre USD 648.12 a USD 6481.25 respectivamente).

ber genérico de seguridad de los datos[13], mientras que otras explícitamente detallan distintas medidas de seguridad a aplicar[14].

En cualquier caso, el potencial adquirente debería incluir en el *due diligence checklist* la revisión de las medidas técnicas y operacionales particularmente adoptadas por la sociedad a ser adquirida para resguardar su información y datos personales, desde controles de acceso, contraseñas, adquisición de productos de software específicos para este fin, si se realizan auditorías periódicas, etc. Dos puntos en especial que consideramos destacables dentro de este rubro son los siguientes: primero, la existencia –o no– de una política de usos de sistemas de IT para los empleados (que a veces se encuentra dentro de la política de privacidad para estos últimos), la cual resulta fundamental en tanto son los empleados de la empresa quienes, a través de dispositivos propios o provistos por la empresa, manejan los datos de la empresa, quienes tienen que cumplir las obligaciones de seguridad de estos últimos y también quienes son sujetos de supervisión al respecto por parte de la empresa, todo lo cual debería estar en esta política; segundo, la contratación o no de pólizas de seguro para incidentes de ciberseguridad.

3.e Incidentes de seguridad de datos personales

Los incidentes de seguridad de datos personales (*data breaches*) ocurren cada vez con mayor frecuencia, producen consecuencias muy gravosas (muchas veces difíciles de dimensionar), sanciones[15] (a veces millonarias) para la empresa que los sufre por parte de la autoridad de aplicación y, además, reclamos de los titulares de los datos afectados. Por ello, constituyen una de las mayores preocupaciones de las empresas, actualmente, cualquiera sea la actividad comercial en que se desempeñen.

Por lo que –en consonancia con las medidas de seguridad señaladas en el punto precedente– resulta conveniente revisar en el *due diligence*: si la empresa ha sufrido incidentes de ciberseguridad durante los últimos años, si los ha reportado (a clientes, a los titulares de los datos, a la autoridad de aplicación de los datos personales, al seguro en caso de contar con una póliza al respecto), si ha formulado denuncias administrativas y/o judiciales al respecto, si existen reclamos pendientes en tal sentido, qué tipo de datos han sido afectados, si se siguió el proceso regulatorio previsto por la ley al respecto, si existen protocolos internos que la empresa ha de seguir para el caso de que sucedan tales incidentes y las medidas adoptadas para intentar evitar que se repitan ataques como los que ya se hubieran producido[16].

3.f Contratos con encargados de tratamiento

Gran parte de los proveedores de la empresa a adquirir actuará como "encargados de tratamiento" (*data processors*) de dicha empresa: figura instituida en la mayoría de las legislaciones sobre datos personales[17]. Estos actúan por cuenta y orden de la empresa que los contrata ("responsable de la base de datos" o "*data controller*") y, como tales, tienen responsabilidades delimitadas por las leyes de datos

13 Art. 9 LPDP Argentina; Art. 9 Ley de Perú. El modelo peruano – afirma Jessica Hondermann– "puede ser considerado de uso mixto pues, si bien la normativa consagra un principio de seguridad, también considera como obligatorio el cumplimiento de ciertas de disposiciones específicas para el tratamiento de los datos personales (gestión de accesos, de privilegios, procedimientos de identificación, registro de interacción con datos lógicos, almacenamiento de información, generación de copias, traslado de documentos, etc.) Además, y de forma complementaria, la autoridad local ha aprobado una Directiva de Seguridad de la Información de carácter orientativo" (comunicación personal, 30 de octubre de 2023).

14 Arts. 24, 25, 32 del GDPR.

15 Dentro de estas multas por el acaecimiento de un *data breach* se encuentran: (i) la multa impuesta por la autoridad de protección de datos personales del Reino Unido en el año 2020 a la cadena hotelera 'Marriott' por un total de £18,400,000 (https://ico.org.uk/media/action-weve-taken/mpns/2618524/marriott-international-inc-mpn-20201030.pdf); (ii) la multa impuesta por la autoridad de protección de datos personales de España en el año 2021 a la aerolínea 'Air Europa' por un total de €600,000 (PS-00179-2020 Resolución de fecha 15-03-2021 Artículo 32 33 RGPD (aepd.es)); (iii) la multa impuesta por la autoridad de protección de datos personales de Irlanda en el año 2021 a 'Meta Platforms Ireland Limited' por un total de €265,000,000 por un *data breach* que derivó en la publicación de datos de 533 millones de usuarios de Facebook y por no aplicar medidas técnicas y organizativas suficientes para proteger los datos personales (Facebook: Meta fined €265m by Irish Data Protection Commission - BBC News); (iv) y la multa impuesta por un total de €746,000,000 por la autoridad de protección de datos personales de Luxemburgo en el año 2021 a Amazon por sendas violaciones a las disposiciones de GDPR, incluyendo aquellas relativas a prevenir los *data breach* (Inline XBRL Viewer (sec.gov)/ Amazon faces $888M GDPR fine (iapp.org)).

16 En el caso de Perú, explica Hondermann, "la obligación de reportar incidentes de seguridad solo es obligatoria para entidades del sector público y para determinados agentes del sector privado (proveedores de servicios digitales del sector financiero, de servicios básicos, de salud y transporte, de internet, de actividades críticas y de servicios educativos). No obstante, existe un proyecto normativo que plantea generalizar el cumplimiento de esta obligación para la integridad del sector privado" (comunicación personal, 30 de octubre de 2023).

17 Art. 28 GDPR, Art. 25 LPDP Argentina, Art. 30 Ley de Perú.

personales que muchas veces son complementadas por obligaciones contractuales adicionales.

Consecuentemente, será determinante evaluar los contratos de la empresa *target* con tales encargados de tratamiento y verificar si contienen cláusulas adecuadas en cuanto al propósito y manejo de tales datos, en especial considerando que el responsable de la base de datos (la empresa *target*) responde frente a terceros por eventuales falencias del encargado de tratamiento y sus eventuales subcontratistas. En las legislaciones de diversas jurisdicciones, a los recaudos contractuales para proveedores (encargados de tratamiento) establecidos por la normativa de *data privacy* deben agregarse requerimientos regulatorios específicos para proveedores de la industria de la que se trata (algo que habitualmente sucede con las entidades financieras, especialmente en lo que refiere a los proveedores de servicios de tecnología informática)[18].

Estos requerimientos contractuales adquieren mayor complejidad cuando el proveedor es una empresa de una jurisdicción distinta a la del país del contratante (la empresa *target*) como se verá más adelante en el presente.

3.g Contratos con clientes

Algo similar a lo reseñado en el punto anterior sucede con los contratos con clientes, en los que–en los últimos años–suele haber cláusulas de datos personales (más o menos detalladas según sea el grado y sensibilidad de los datos intercambiados entre las partes). Naturalmente, cuanto más y mejor detallado en el contrato se encuentren la finalidad de tratamiento, las medidas de seguridad adoptadas, los efectos en distintos supuestos que involucren a tales datos, etc.; menores serán las potenciales contingencias.

3.h Transferencia internacional de datos

Casi todo el derecho comparado de *data privacy* trata separadamente las transferencias internacionales de datos personales. Con la incorporación de la tecnología e internet como factor indispensable del funcionamiento empresarial (independientemente de tamaño y rubro de la empresa y con el auge de "la nube" en particular (con datos almacenados en distintos servidores ubicados a lo largo de distintas jurisdicciones), las transferencias internacionales de datos ocurren constantemente, todos los días, casi sin que nos demos cuenta. Ello en nada obsta a que las empresas deben cumplir los recaudos regulatorios a tal efecto bajo la pena de ser sancionadas por tal incumplimiento. La mayor o menor rigurosidad de tales recaudos dependerá generalmente de que los países a donde se importen los datos tengan o no legislación 'adecuada' en materia de datos personales, lo cual es determinado por la legislación del país de la empresa exportadora.

Por eso, a los recaudos de los contratos con terceros comentados en las secciones 3.f. y 3.g. del presente, deben agregarse los requerimientos para transferencias internacionales en la medida en que el tercero se encuentre en otra jurisdicción o que la operación suponga una transferencia transfronteriza de datos personales[19], en especial si se realizará con destino a países sin "legislación adecuada" de datos personales. El cumplimiento de estos requisitos adquiere mayor relevancia si la empresa a adquirir es parte de un grupo multinacional y/o mantiene relaciones contractuales con la Unión Europea u otras jurisdicciones que prevean la aplicación extraterritorial de sus leyes de datos personales. El cumplimiento de esta obligación en Perú, afirma Hondermann, "viene acompañado con una obligación de carácter más formal, conforme a la cual, de realizarse alguna modificación en la entidad y el país receptor de los datos, ello deberá ser comunicado a la autoridad local" (comunicación personal, 30 de octubre de 2023).

3.i Reclamos de titulares de datos y/o de terceros

Como cualquier reclamo contra la compañía, los reclamos de los titulares de los datos (por ejemplo, para que se supriman, actualicen o modifiquen sus datos) constituyen una posible contingencia para la compañía destinataria de los mismos. Consecuentemente, habrá que constatar si existen, fueron respondidos, quedaron terminados, etc. En líneas muy generales, este tipo de reclamos no suele constituir una contingencia de gran envergadura económica para la compañía, salvo que se trate de acciones de clase, reclamos subsumidos dentro de otros reclamos que involucren otras cuestiones (laborales, societarias, etc.) o bien denuncias ante la

18 Comunicaciones A6354, A6375 y A7724 del Banco Central de la República Argentina.

19 Art. 44 GDPR y ss. Art 12 LPDP Argentina reglamentado por el Decreto 1558/2001, Disposición AAIP 60/2016 y Resolución AAIP 198/2023. Art 15 Ley de Perú.

autoridad de aplicación, cuestión que veremos en el punto siguiente.

Es importante considerar que en muchos casos este tipo de reclamos debe analizarse a la luz de la normativa de datos personales juntamente con normas de otras áreas del derecho, dependiendo de quién provengan y/o el tipo de datos objeto del pedido. Por ejemplo, si el reclamo proviene de un socio, habrá que analizar el derecho de información del socio previsto en la legislación societaria de la jurisdicción que se trate; si el reclamo proviene de un empleado o exempleado, habrá que analizarlo también bajo los preceptos de la ley de contrato de trabajo. También, habrá que analizar si revelar los datos del titular que se reclaman puede involucrar revelar otros datos que perjudicarían a terceros que estén amparados por normativa de secreto profesional (por ejemplo, de abogados o médicos) o que simplemente no son de titularidad de quien los pide. Esta controversia es bastante común cuando se reclaman correos electrónicos (*e-mails*) remitidos por empleados de la compañía que generalmente involucran a varias partes.

3.j Actuaciones ante la autoridad de aplicación de datos personales

La existencia y el estado de procesos administrativos activos ante la autoridad de aplicación son determinantes para evaluar las contingencias de la compañía, habida cuenta que de ellos pueden surgir sanciones para esta última. Lógicamente, en el *due diligence* habrá que relevar su grado de avance y determinados parámetros (antecedentes de la compañía y normativa sobre graduación de sanciones) para prever la probabilidad de multas y su cuantía.

Además, afirma Hondermann, en el caso de Perú, lo siguiente:

> El análisis de contingencias en materia de datos personales puede generar que se analicen infracciones directamente vinculadas que provienen de otras áreas de práctica como protección al consumidor. Así, por ejemplo, mientras la normativa de datos personales sanciona el tratamiento de los datos personales sin el consentimiento libre, expreso, inequívoco, previo e informado del titular de los datos; la normativa de protección al consumidor sanciona emplear *call centers*, sistemas de llamado telefónico, envío de SMS a celular o de correos electrónicos masivos a aquellos números telefónicos y correos de consumidores que no hayan brindado su consentimiento previo, informado, expreso e inequívoco para la utilización de esta práctica comercial. (comunicación personal, 30 de octubre de 2023)

3.k Evaluaciones de impacto de datos personales

Las legislaciones más modernas en materia de *data privacy* prevén la obligación de realizar evaluaciones de impacto de datos personales (Parlamento Europeo, 2016, p. 35)[20] precio a la implementación de determinadas actividades o lanzamiento de ciertos productos considerados riesgosos o que puedan afectar una gran cantidad de datos o ciertas categorías de datos (por ejemplo, datos sensibles). De ser este el caso en la jurisdicción aplicable a la potencial transacción, habrá que relevar si tal evaluación fue efectuada de acuerdo en tiempo y forma de acuerdo a la normativa en cuestión; y, en caso negativo, las posibles sanciones por el incumplimiento.

4. Implementación *(closing)* del contrato de M&A: cláusulas de *data privacy*

Para perfeccionar la operación de fusión o adquisición, las partes deberían suscribir el respectivo contrato en el cual, entre muchas otras cuestiones, deberían existir cláusulas que regulen todo lo atinente al impacto que ello tendrá en las bases de datos de la empresa adquirida y las obligaciones de las partes al respecto. Como adelantamos al inicio, tales cláusulas diferirán según la actividad de las empresas y de la naturaleza jurídica de la transacción en cuestión: las previsiones serán distintas según se trate de una fusión societaria, de la adquisición de un paquete accionario o de la compra

20 Artículo 35 GDPR. En Argentina, si bien la LPDP Argentina no incluye una previsión específica al respecto, la AAIP publicó junto con la autoridad de protección de datos personales de Uruguay en el año 2020 la "Guía de Evaluación de Impacto en la Protección de Datos", la cual puede ser utilizada por las partes involucradas en el tratamiento de datos personales para llevar a cabo la misma. Si bien dicha guía fue concebida como un documento de consulta, recientemente la AAIP solicitó a la compañía WorldCoin que le indique si realizó las evaluaciones de impacto respectivas utilizando la presente guía. Adicionalmente, el Convenio 108+ en su art. 12 establece la obligación en cabeza de los Estados parte de requerir a los *controllers* y *processors* la realización de dicha evaluación. El mencionado Convenio 108+, en Latinoamérica, fue firmado y ratificado solamente por Argentina y Uruguay (Full list - Treaty Office (coe.int)). En el caso de Perú, la Ley de Perú no incluye dicha previsión, pero –señala Hondermann– "el Proyecto de Nuevo Reglamento de dicha norma, la considera como una obligación de cumplimiento facultativo por parte de los titulares de los bancos de datos".

de una unidad de negocios o fondo de comercio, por citar algunas. Identificaremos seguidamente las cuestiones sobre datos personales que –ya sea entre las declaraciones y garantías, ya sea en cláusulas específicas– deberían incluirse en este tipo de contratos, adaptadas según sea la estructura jurídica del negocio de M&A a realizarse.

4.a Notificaciones

Casi todas las transacciones de fusión y/o adquisición involucran notificaciones de distinto tipo a terceros, incluyendo organismos gubernamentales. Desde la perspectiva de *data privacy*, las mismas dependerán de su estructuración.

Si, por ejemplo, se adquiere un porcentaje accionario de una sociedad, probablemente nada deba ser notificado ni a los titulares de los datos ni a la autoridad de aplicación de datos personales, ya que el responsable de tales datos seguirá siendo la misma empresa, independientemente del cambio en su composición accionaria. Si, en cambio, se trata de una fusión o la adquisición de una 'unidad de negocio' (que carece de personería jurídica como tal), probablemente sí deba ser notificado –o incluso puede llegar a requerirse consentimiento previo–, ya que habrá técnicamente una 'cesión de datos personales' y cambiará el responsable de la base de datos (mis datos personales, que antes tenía la sociedad A, ahora pasará a detentarlos la sociedad B). Habrá que estar atentos a la normativa de las jurisdicciones involucradas en la operación porque muchas legislaciones, como la peruana, contemplan expresamente el caso de cesión de bases de datos por fusión o adquisición del responsable de las mismas. La Ley de Perú, por ejemplo, prevé estos supuestos y permite realizarlos sin requerir consentimiento previo de los titulares de los datos involucrados, pero con la obligación de notificarlos de dicha operación (Congreso de la República del Perú, 2011, p. 4)[21]; y la autoridad de aplicación de datos personales de Perú se ha expedido más detalladamente respecto del momento en que debe efectuarse dicha notificación[22]. Estas consideraciones deben tomarse en cuenta y pactarse expresamente entre las partes de la transacción, incluyendo el modo de su implementación (por ejemplo, si deben realizarse notificaciones, qué parte las realizará, por qué medio, en qué tiempo, cómo debe acreditarlo ante la otra parte, etc.).

4.b Declaraciones y garantías

Las declaraciones y garantías sobre datos personales de la compañía a adquirir deberían reflejar, esencialmente, el resultado del *due diligence* previamente efectuado.

4.c Responsabilidades

La inexactitud o falsedad de las declaraciones y garantías otorgadas acarreará la responsabilidad de la parte declarante, quien deberá responder por los daños y perjuicios ocasionados con motivo de dicha inexactitud o falsedad. Por lo tanto, ambas partes deberán cerciorarse de que las declaraciones y garantías otorgadas se ajusten a la realidad de la operación, debiendo revisarse al momento del *closing*, el mantenimiento de dichas declaraciones y garantías.

Asimismo, debe definirse con precisión el alcance de las responsabilidades asumidas por las partes; es decir, acerca de qué personas están involucradas, de la naturaleza de los datos proporcionados, del uso de los datos proporcionados, de los reclamos recibidos respecto de los datos y su manejo deberá cada parte responder. Por lo tanto, al momento de instrumentar el contrato, resulta necesario que las partes definan –conforme lo detallado precedentemente– dicho alcance a los efectos de minimizar las potenciales contingencias que podrían resultar del M&A.

21 El art. 18 de la Ley de Perú reformado por el Decreto Legislativo N°1353, permite la transferencia sin necesidad de un consentimiento posterior del titular del dato en caso de una transferencia resultante de una fusión, adquisición de cartera o supuestos similares al prescribir "Si con posterioridad al consentimiento se produce la transferencia de datos personales por fusión, adquisición de cartera, o supuestos similares, el nuevo titular del banco de datos debe establecer un mecanismo de información eficaz para el titular de los datos personales sobre dicho nuevo encargado de tratamiento".

22 A través de la Opinión Consultiva 241-2017, la Dirección Nacional de Protección de Datos Personales de Perú se expresó acerca del alcance del mencionado art. 18, indicando que ello no implica la solicitud de un nuevo consentimiento al titular del dato, el cual debe ser recolectado previo al tratamiento siempre que no se enmarque en una excepción del art. 14 de la Ley de Perú, sino únicamente el deber del responsable de tratamiento de informar al titular del dato sobre dicha transferencia. La mentada Dirección Nacional de Protección de Datos Personales de Perú en la antedicha Opinión Consultiva 241-2017 indica que se le debe informar al titular del dato *"*una vez que se ha tomado la decisión de establecer vínculo con un nuevo encargado o de realizar la transferencia por fusión, adquisición de cartera o supuestos similares pero de forma anterior a la transmisión de datos personales al nuevo encargado o nuevo titular del banco de datos, toda vez que el deber de informar debe realizarse de forma previa al tratamiento de datos personales*"*. En cuanto a los medios para comunicar ello al titular del dato, la Opinión Consultiva 241-2017 permite el uso de los medios habituales de comunicación con el titular del dato para informarles la presente.

4.d Indemnidades específicas

Este punto interesa a las partes involucradas en la transacción, dado que definirá el alcance de la misma respecto a los eventuales reclamos de diversa índole (laborales, administrativos, judiciales, por nombrar algunos) susceptibles de ser interpuestos por terceros.

En particular, en lo referido a este aspecto, las partes deberán pactar indemnidades específicas vinculadas; por ejemplo, al manejo de los datos por parte del *target*, a la posible existencia de procedimientos en trámite y/o finalizados llevados adelante por las autoridades gubernamentales a raíz de reclamos interpuestos o iniciados de oficio por sendas autoridades y a las sanciones que podrían ser impuestas al *target* consecuencia de su accionar.

También se deberá negociar el límite de dicha indemnidad, la cual, por lo general, suele extenderse a los accionistas y directores del *target*.

5. Obligaciones *post-closing*

Las obligaciones posteriores al perfeccionamiento contractual de la fusión o adquisición estarán mayoritariamente vinculadas a controlar el efectivo cumplimiento de todo lo previsto en dicho contrato: esto interesa a ambas partes, ya que, en líneas generales, ambas pueden llegar a ser solidariamente responsables frente a terceros independientemente de cuál haya sido la eventual incumplidora. Ello sin perjuicio de las cláusulas de indemnidad y repetición que hayan previsto al respecto: válidas entre las partes de la operación, pero inoponibles a terceros.

Estas obligaciones variarán de acuerdo a la naturaleza del M&A realizado. Dentro de las obligaciones más comunes, se encuentra la asistencia al comprador por parte del vendedor para integrar la estructura del *target* adquirido a la matriz del comprador. Esta integración puede llevarse a cabo a través de un análisis de cuáles serán las actividades en las que el comprador requerirá asistencia, junto con el correspondiente destino de recursos por parte del vendedor para asistir en el transcurso de dicha integración.

Sobre los datos ubicados dentro de los sistemas del *target*:

> ¿Se integrarán a la matriz del comprador, o se mantendrán por separado en dos sistemas paralelos? ¿Qué parte cuenta con políticas de privacidad más robustas para aplicar? ¿Cómo se podrán unificar las políticas? ¿Hay nuevas jurisdicciones en donde se almacenarán o transferirán datos personales como consecuencia del M&A? (Habash et al., 2016)

Estos son solo algunos de los interrogantes que se plantean al momento de efectuar la integración en materia de *data privacy*, los cuales deberán ser resueltos por las partes. Una vez finalizada la misma, las partes pueden pactar un análisis acerca del resultado de dicha integración con el objetivo de visualizar posibles aspectos no alcanzados en la misma y posibles riesgos asociados a la integración.

Es posible que –producto de la integración– las partes individualicen ciertos riesgos a los que dados los tiempos de las partes o a la baja probabilidad de ocurrencia no hayan podido ser abordados dentro de las etapas previas al *closing* y a la celebración del contrato de M&A. Es por ello que las partes deberán acordar –conforme la integración llevada adelante y su resultado– la existencia y aplicación de posibles medidas que permitan mitigar dichos riesgos y sus consecuencias en caso de que ocurran, tales como la obligación en cabeza de los órganos de gobierno y administración del *target* de realizar determinadas actividades en materia de *data privacy* para cumplir con el objetivo antes dicho y de esa manera minimizar la eventual responsabilidad frente a terceros de las partes de la operación. Estas obligaciones resultan de especial importancia en caso de que el comprador no adquiera la totalidad de las acciones o bien no haya absorbido –en caso de una fusión– la totalidad de los negocios llevados adelante por el *target*.

Una vez finalizadas la transacción y la correspondiente instrumentación del contrato respectivo, ¿debe el vendedor eliminar los datos del *target* que tenía en su poder? En lo que respecta a *data privacy*, las legislaciones en la materia imponen la obligación de eliminar los datos recolectados una vez que ellos hayan dejado de ser útiles para los fines que han sido recabados[23], incluso existiendo previsiones que imponen un plazo determinado[24]. Sin embargo, este principio colisiona con disposiciones de otras áreas del derecho (tales como el derecho civil), que permiten expresamente que los datos personales sean conservados por un tiempo

23 Art. 5 inciso "e" GDPR. Art. 4 inciso 7 LPDP Argentina. Art. 8 Ley de Perú.

24 Arts. 25 inciso "2" y 26 LPDP Argentina.

mayor al estipulado en las legislaciones de *data privacy.*

Tal es el caso del Código Civil y Comercial argentino –el cual es una norma de carácter federal–, que habilita la conservación por hasta 10 años, contados a partir de la fecha que tengan, de cualquier instrumento respaldatorio (Congreso de la Nación de Argentina, 2014, art. 328 inciso c). Por lo tanto, ¿todo aquel instrumento en donde se encuentren asentados los datos personales que fueron objeto de la transacción debe ser eliminado inmediatamente luego de finalizada la misma, dado que ya habrían dejado de ser útiles o deben ser conservados por un plazo mayor (por ejemplo, el señalado supra)?

El mismo interrogante sucede en caso de que el *target* de la transacción haya sido un establecimiento sanitario. En lo referido a Argentina, la Ley de Derechos del Paciente N°26.529 indica que las historias clínicas deben ser almacenadas durante el plazo mínimo de 10 años desde la prescripción liberatoria de la responsabilidad contractual (Congreso de la Nación de Argentina, 2009)[25].

En el caso de Perú, Hondermann señala lo siguiente:

> La figura es similar pues, en función del negocio al que se haya dedicado el *target*, la normativa podría establecer plazos específicos de conservación de la información de los trabajadores. Así, por ejemplo, en general, la legislación laboral prescribe que los registros de enfermedades ocupacionales se deben conservar por un período de 20 años, pero para actividades de alto riesgo para la salud de los trabajadores se indica que las historias clínicas deben conservarse, como mínimo, por 40 años. (comunicación personal, 30 de octubre de 2023)

En consecuencia, se debería prever en el contrato mediante el cual se instrumente el M&A la obligación de establecer un plazo por el cual deberá el vendedor mantener la documentación con posterioridad al cierre de la transacción.

6. Conclusión

Las regulaciones en materia de *data privacy* presentan un gran dinamismo como respuesta a la constante evolución tecnológica y la consiguiente aplicación de las mismas en las estructuras de todas las compañías del mundo.

Es por ello que las consideraciones legales abordadas en el presente no serán las únicas el día de mañana, sino que las mismas se actualizarán de la mano del antedicho dinamismo legislativo, abarcando potencialmente áreas no contempladas en la actualidad.

Referencias bibliográficas

Congreso de la Nación Argentina. (30 de octubre de 2000). *Ley 25.326 de 2000*. https://www.oas.org/juridico/pdfs/arg_ley25326.pdf

Congreso de la Nación Argentina. (21 de octubre de 2009). *Ley 26.529 de 2009. Derechos del Paciente en su Relación con los Profesionales e Instituciones de la Salud*. https://servicios.infoleg.gob.ar/infolegInternet/anexos/160000-164999/160432/texact.htm

Congreso de la Nación Argentina. (8 de octubre de 2014). *Ley 26.994 de 2014*. Código Civil y Comercial de la Nación. https://www.argentina.gob.ar/normativa/nacional/ley-26994-235975/actualizacion

Congreso de la República del Perú. (3 de julio de 2011). *Ley N°29733 de 2011*. https://www.leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf

Dirección Nacional de Protección de Datos Personales. (10 de abril de 2015). *Disposición 18 / 2015*. https://servicios.infoleg.gob.ar/infolegInternet/anexos/245000-249999/245973/norma.htm

Habash, R.; Janssen, B.; Knouff, M. (22 de agosto de 2016). *Data Privacy and security issues in M&A transactions: Part two.* https://iapp.org/news/a/data-privacy-and-security-issues-in-ma-transactions-part-two/#

Parlamento Europeo. (27 de abril de 2016). *Reglamento (UE) 2016/679 de 2016*. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:02016R0679-20160504

25 Art. 18 Ley N°26.529.