UNIVERSIDAD DE CIENCIAS EMPRESARIALES Y SOCIALES

Título de la tesis:

LA GARANTÍA DE LOS DERECHOS A LA INTIMIDAD Y PRIVACIDAD *POST MORTEM* A LA LUZ DE LOS SISTEMAS JURÍDICOS DE PROTECCIÓN DE DATOS PERSONALES EN ARGENTINA Y BRASIL

Tesis de Doctorado en Derecho con orientación en Derecho Privado

Autor
João Paulo Rodovalho de Oliveira

Director de la Tesis
Dr. Claudio Schifer

Buenos Aires, febrero de 2021

ÍNDICE

Introducción

La revolución en el universo de las tecnologías de la información y las comunicaciones produjo al mismo tiempo significativos beneficios y múltiples interrogantes para la humanidad. Conceptualmente, el surgimiento de la Industria 4.0 y la Sociedad 5.0 nos señala que la evolución de la tecnología se encuentra en permanente movimiento, siendo imprevisibles los límites de los caminos que se transitan, la transformación de los hábitos y su impacto en la dinámica social.

Aquello que no pudo ser integrado al progreso tecnológico ha sido reemplazado gradualmente por herramientas y comportamientos sociales de la era digital. En este contexto, la producción, transferencia y almacenamiento de datos de los más variados orígenes son hechos que ya no se pueden desvincular de la rutina humana, causando en las personas una dependencia cada vez mayor del empleo de la informatización, incrementada intensamente en el mundo entero, a partir de la pandemia por coronavirus/Covid-19.

Giardelli (2012, p. 16), ilustrando lo expuesto afirma que las personas se desplazan por el tejido social como si estuvieran en piloto automático, como viajeros robotizados programados para no cuestionar, no hablar, no oír. Sólo sintonizar y conectar.

La información volcada en los dispositivos conectados a Internet y en diversas redes, de manera continua, a veces inconsecuente e inconsciente, hace que las personas transmitan al mundo virtual prácticamente todo sobre sus vidas, generándose así la personalidad del usuario; información que suele alojarse en una amplia variedad de bancos de datos. Esta regla es aplicable también a los sectores económicos y gubernamentales que, a diferencia de la mayoría de las personas, procuran blindarse cada vez más con el objeto de proteger la información que registran, perteneciente al mismo tiempo, al mundo real y virtual.

No es casualidad entonces que en los últimos años comenzara una carrera mundial para la protección de datos procurando gran parte de las naciones la adecuación de sus ordenamientos jurídicos a la revolución tecnológica y a la

virtualización de la vida, advirtiéndose en la mayoría de los continentes la creación y actualización de la legislación sobre la protección de datos personales.

Queda claro que los seres humanos son, en síntesis, las figuras más vulnerables en este mecanismo de virtualización de las relaciones personales. Aquello que conversan, buscan, compran, transfieren, publican y ocultan en Internet es sumamente valioso para el mundo virtual, pues sobre estos datos resulta posible indagar en sus vínculos familiares, económicos, tributarios, sociales, afectivos, sindicales, religiosos, históricos, tecnológicos, policiales y judiciales, por citar ejemplos; extendiéndose el concepto de "vida virtual", a la salud y sexualidad, entre otros ámbitos de la personalidad.

Según Saltor (2013):

> [L]as personas han tenido que adaptarse a una sociedad en la que cada vez son más reducidos los espacios privados. Por este motivo en la actualidad la lucha por la defensa de la vida privada se ha transformado en la lucha por la defensa y control de la información personal que concierne a cada uno y que revela los comportamientos y hábitos de cada persona, incluso los más íntimos. (p. 25)

La interpretación, a partir de estas palabras, es que los conceptos "intimidad y privacidad" necesitan de una amplia atención en el ámbito de la innovación legislativa internacional sobre la protección de datos, la que debe abarcar, también, el tratamiento de los datos e información de las personas después de su fallecimiento. La preocupación por la protección de estos datos se extiende una vez finalizada la vida, ya que aunque la personalidad jurídica se ha extinguido los datos y la información sobre la persona fallecida continúan existiendo en el mundo virtual. Es decir, su perfil virtual no se apaga con el fin de la vida.

En este punto, se sostiene que es de gran importancia investigar el alcance de la protección dada por los ordenamientos jurídicos a los datos que transitan por Internet *post mortem*. Argentina y Brasil, por ejemplo, no han producido una legislación específica sobre la utilización de los datos e información de las personas fallecidas alojadas en Internet. Por este motivo, dichos países fueron elegidos para el objeto de este estudio, ya que utilizan normas generales sobre el

uso de Internet y sobre la protección de los derechos personalísimos para garantizar, por ejemplo, la intimidad y privacidad en tiempos de revolución tecnológica.

De los estudios preliminares emergió la convicción sobre la importancia de la investigación, pues la problemática no ofrece respuestas concretas, en función de la ausencia de normas específicas y la escasa judicialización de la temática en curso. Por tal motivo, el presente trabajo trata diversos aspectos de interés científico sobre los derechos personalísimos, principalmente los relacionados con el universo virtual. Se advierte, igualmente, que la doctrina tiene poca preocupación por el tema elegido, requiriéndose profundizar en los aspectos más importantes que surgen en torno al mismo.

En este contexto, la pregunta a la que se intenta dar respuesta en la investigación es: **¿En qué medida los sistemas jurídicos de protección de datos personales en Argentina y Brasil garantizan la intimidad-privacidad de las personas después del fallecimiento?**

La hipótesis que se sostiene es que el derecho a la intimidad y privacidad en Argentina y Brasil, respecto a los datos personales de las personas fallecidas alojadas en Internet, es insuficientemente tutelado. Por ello, a través de la presente tesis de doctorado se ofrece una solución jurídica para la regulación de la utilización de los datos de las personas fallecidas guardados en Internet en Argentina y Brasil, con miras a que sea de utilidad de jueces y legisladores, sirviendo de fuente de estudio para futuras investigaciones y proyectos normativos en la especialidad.

Para avanzar en esta dirección, en el Capítulo I se da cuenta del Estado del Arte, haciendo una comparación entre las normas jurídicas, la jurisprudencia y la doctrina de Argentina y Brasil acerca de la protección general sobre los datos personales.

En el Capítulo II se desarrollan los sistemas jurídicos sobre la protección de los datos personales en los países citados que protegen la intimidad y privacidad de los usuarios de Internet.

En el Capítulo III se señala cómo la protección de los datos personales existentes en Argentina y Brasil, garantizan los derechos a la intimidad y privacidad de las personas vivas. La idea es poder realizar un comparativo de este objetivo con el problema principal del presente trabajo doctoral. Al mismo tiempo es demostrada la importancia de los datos personales en el contexto de la revolución tecnológica, por lo que se analiza el valor económico de este tipo de información y a quiénes interesa; investigando también las políticas de registro y almacenamiento de datos de las redes sociales más utilizadas en Argentina y Brasil.

En el Capítulo IV comienza el direccionamiento de la investigación hacia el problema principal, pasando a dar cuenta de la utilidad de los datos de las personas fallecidas alojados en Internet. En este punto se trata de explicar en qué medida se comportan Argentina y Brasil en el tratamiento jurídico de los datos personales de las personas fallecidas guardados en Internet.

En el Capítulo V se aborda una propuesta jurídica con el objeto de salvaguardar la utilización de los datos personales en Internet, después del fallecimiento, a partir de un análisis de la normatizacíon europea, especialmente de España y Francia. La intención es la de proponer una posible solución jurídica a la problemática central del presente trabajo, para su aplicación en la Argentina y Brasil.

Capítulo I: Estado del arte

Los derechos de la personalidad no han escapado a la disrupción causada por el avance de la tecnología en la sociedad de la información, ya que los sistemas que tradicionalmente garantizaban la inviolabilidad de institutos como la intimidad y privacidad ya no son tan efectivos como antes. Las acciones íntimas y privadas de las personas dejan huellas que ahora se eternizan en los medios tecnológicos, demandando una protección moderna y alineada con los nuevos comportamientos sociales. Es por ello, que el presente trabajo prestará especial atención a los derechos de la personalidad más vulnerables a la revolución tecnológica: privacidad e intimidad.

La regulación europea, que influye fuertemente en las leyes de Argentina y Brasil en materia de protección de datos personales ha sido de avanzada en el resguardo de las garantías individuales. Encuentra su sustrato jurídico en la protección de los derechos fundamentales a la intimidad y privacidad que garantiza la Convención Europea de Derechos Humanos del año 1950 en su art. 8º (Faliero, 2018, pp. 57-58).

Sin embargo, no debemos olvidar la Declaración Universal de Derechos Humanos de 1948, que establece en el artículo 12, que “nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques”.

Además de la Declaración Universal de Derechos Humanos citada, la Declaración Americana de los Derechos y Deberes del Hombre (artículo 5), el Pacto Internacional de Derechos Civiles y Políticos y su Protocolo Facultativo (artículo 17), la Convención sobre los Derechos del Niño (artículo 16), y la Convención Americana sobre Derechos Humanos (artículo 11) receptan dicho derecho; tratados que han sido incorporados al texto de la Constitución de la República Argentina (artículo 75, inciso 22), gozando de jerarquía constitucional.

De acuerdo con Villegas Carrasquilla (2012), este tipo de reglamentación se fundamenta, principalmente, en el derecho de cada individuo a su intimidad. Sin

embargo, la noción de intimidad y vida privada, su fundamento como derecho y la manera de regularlo y protegerlo varían de región en región, de país en país (p. 127).

Bidart Campos (2014), diferenciando tales institutos, afirma, que la privacidad sería la posibilidad irrestricta de realizar acciones privadas -que no dañan a otros- por más que se cumplan a la vista de los demás y que sean conocidas por éstos. Se trata siempre de una zona de reserva personal, propia de la autonomía del ser humano. Y la intimidad sería la esfera personal que está exenta del conocimiento generalizado de terceros (p. 213).

Silva (2018, p. 210) sostiene que no es fácil distinguir la privacidad de la intimidad. Aquella, en última instancia, integra la esfera íntima de la persona, porque es repositorio de secretos y particularidades del fuero moral e íntimo del individuo. Según Piton (2017, párr. 66), la intimidad no se debe confundir con la vida privada, ya que aquella guarda secretos y deseos íntimos que solo el individuo conoce. Por otro lado, la vida privada es menos secreta.

A lo largo de este trabajo, la intimidad y privacidad se enfrentarán a los avances tecnológicos, presentándose los riesgos, intereses y protecciones existentes relacionadas con estos derechos. La protección de los datos personales será la materia en evidencia, ya que ellos son los principales agentes que ponen en peligro no solo a los institutos en foco, sino a otros derechos de la personalidad.

De acuerdo con las enseñanzas de Tomasevicius Filho (2016):

> En menos de veinte años de uso comercial, Internet ha cambiado muchos aspectos de la vida humana. El principal de ellos fue la expansión del conocimiento y el acceso a la cultura. Basado solo en los cincuenta años anteriores a la apertura de Internet, la información se difundió a través de libros impresos. Las búsquedas escolares se realizaron en enciclopedias y almanaques, disponibles, respectivamente, en bibliotecas y quioscos. En Internet, estos materiales pronto perdieron terreno en las *homepages* con sus costos muy bajos de divulgación de información. Debido a la facilidad de acceso en cualquier momento y lugar, la velocidad de transmisión del conocimiento aumentó casi hasta el infinito. (p. 269).

Al aumentar la capacidad y las oportunidades de acción de los individuos, los medios de comunicación e información aumentan, en la misma dimensión, los riesgos a los que están sujetos los individuos (Hartmann; Wimmer, 2011, p. 21).

Es a partir de estas declaraciones que se trata de comprender la evolución del almacenamiento y la protección de datos y su impacto en la vida social y privada de los seres humanos. Esta puede ser la preocupación más intensa de la humanidad por las generaciones presentes y futuras (Rodovalho, 2021, p. 26). Becerra y Zárate (2015, p. 218) indican que la sobreexposición de lo privado que genera la tecnología a los que están expuestos en las redes personales, profesionales y sociales en diversos casos permite que se vulnere la dignidad y que se cause daño a la integridad de las personas.

Westin (1970) explica que por diversas razones, como la ampliación de la complejidad del sistema industrial, la burocratización de los sectores público y privado y la transformación de las ciencias sociales, nos convertimos en la sociedad que más datos personales ha generado en la historia de la humanidad, como lo muestran las diversas bases de datos en los más variados sectores, citándose, entre otros, registros estatales y de entidades privadas (pp. 158-159).

Aunque lejos de la declaración de Westin, el almacenamiento de datos no es una preocupación generada en la sociedad que vive la revolución tecnológica. Es evidente que la preocupación de esa época giraba en torno al almacenamiento antes mencionado, especialmente con fines burocráticos (Rodovalho, 2021, p. 26). Bennett (1992, p. 43) afirma que el uso masivo de datos personales de la segunda mitad del siglo XX puede asociarse con dos características principales del Estado postindustrial: la burocratización –de los sectores público y privado– y el desarrollo de las tecnologías de la información.

La disciplina de la protección de datos personales surge dentro de la sociedad de la información como una posibilidad de proteger la personalidad del individuo contra los riesgos potenciales que puede causar el procesamiento de datos personales. Su función no es proteger los datos *per se*, sino la persona que los posee (Mendes, 2014, p. 32).

Placzek (2006) explica que, en los papeles sociales más diversos, como contribuyente, paciente, trabajador, beneficiario de programas sociales o consumidor, los ciudadanos procesan sus datos día a día. La vigilancia deja de ser esporádica y se vuelve cotidiana. El uso masivo de datos personales por parte de organismos estatales y privados desde las tecnologías de la información avanzadas presenta nuevos desafíos para el derecho a la privacidad. La combinación de varias técnicas automatizadas permite la obtención de informaciones confidenciales de los ciudadanos y la construcción de verdaderos perfiles virtuales, que se convierten en la base para la toma de decisiones económicas, políticas y sociales (p. 2).

Un ejemplo de esto es la técnica de construir perfiles personales mediante los cuales se pueden tomar decisiones importantes sobre los consumidores, los trabajadores y los ciudadanos en general, afectando directamente la vida de las personas e influyendo en su acceso a las oportunidades sociales (Mendes, 2014, p. 34).

Desde este punto de vista y para permitir una respuesta adecuada a los desafíos sociales derivados de la revolución tecnológica, enseña Pérez Luño (1996, p. 10), es esencial que la teoría del derecho sea reconstruida hasta el punto de comprender y resolver los nuevos problemas que enfrenta el hombre en la era de la información. Es importante que los juristas adquieran la capacidad de reflexionar de manera crítica y responsable sobre las dificultades derivadas de la tecnología, lo que Vittorio Frosini llamó "conciencia tecnológica".

Aunque la idea de Frosini (*apud* Pérez Luño, 1996, p. 10) ha sido incorporada por juristas de todo el mundo, demuestra la imposibilidad de los sistemas jurídicos de mantenerse al día con la inserción meteórica de la tecnología en la vida social. Más allá que existe una carrera en el mundo para regular la protección de datos, es un hecho que la conciencia tecnológica de los juristas no ha podido acomodar los nuevos y numerosos problemas creados por la revolución tecnológica.

El punto de partida de esta investigación es la crisis de los derechos de la personalidad, especialmente los derechos a la intimidad y privacidad, que han sido

profundamente impactados por la revolución tecnológica. Según Schwab (2016, p. 15), hoy se enfrentan una gran diversidad de desafíos fascinantes; entre ellos, la más intensa e importante es la comprensión y conformación de la nueva revolución tecnológica, que implica nada menos que la transformación de toda la humanidad. Es el comienzo de una revolución que modificará profundamente la forma de vida, advirtiéndose actualmente dichos cambios, en la educación, el trabajo, la salud, la seguridad, el entretenimiento y las relaciones humanas. En su escala, alcance y complejidad, se considera que la cuarta revolución industrial no se parece a nada que haya experimentado la humanidad.

En esta etapa de disrupción que atraviesa el mundo, se generan innumerables y novedosas situaciones, sin que gobiernos, instituciones, empresas y ciudadanos sepan actuar adecuadamente. Esta realidad también involucra la intimidad y la privacidad, ya que estos derechos están en riesgo por la revolución tecnológica. La doctrina clásica, mencionada en los capítulos siguientes, continúa conceptualizando tales derechos de la personalidad de la misma manera que lo hizo hace décadas.

Es natural que las situaciones creadas por la abrupta inserción de la tecnología en la vida cotidiana aún no tengan una regulación. Son contados los momentos en que la ley es capaz de anticipar los hechos sociales. Por eso no es apropiado esperar que el Derecho se mueva a la misma velocidad que las tecnologías digitales.

Pero lo cierto es que, aunque la realidad digital sea nueva, no es algo que se haya creado de la noche a la mañana. Comenzó en la tercera revolución industrial, y solo se intensificó en las últimas dos décadas. No es casualidad que existan normas que regulen episodios sociales vinculados a la tecnología desde principios de los años 90.

De acuerdo con Zampier (2021, p. 1), la dogmática jurídica ha ignorado en gran medida este nuevo escenario social, insistiendo más a menudo en trabajar hipótesis que remitan a una sociedad basada únicamente en la realidad y no en la virtualidad. Esta cautela, o incluso omisión del Derecho sobre las influencias tecnológicas, favorece la creación de un espacio hermenéutico para un

pensamiento crítico de nuestra ciencia, sea bajo el sesgo de la formulación de normas adecuadas, sea por la aplicación judicial de las normas existentes.

Lo que motiva este trabajo, entonces, es la ausencia de regulaciones específicas sobre intimidad y privacidad *post mortem* en un mundo completamente nuevo, donde los conceptos y normas tradicionales ya no son garantes de la seguridad de antes. Esta tesis surge en un momento en que los derechos de la personalidad todavía están regulados mayormente por normas antiguas, siendo las más recientes de por sí incompletas. En la misma línea, los poderes judiciales no se han abocado al tema, y la doctrina, si bien es la más atenta a la nueva realidad, observa y propone soluciones abstractas al respecto.

No se puede negar, por supuesto, la amplitud de los problemas jurídicos relacionados con los derechos de la personalidad *post mortem*. Es evidente que no solo la intimidad y la privacidad se ponen en riesgo con el final de la vida. Por caso, otros derechos personalísimos, como la imagen, el nombre, el honor y la dignidad de la persona fallecida, merecen ser atendidos, si es que proyectamos para estos derechos, igual protección jurídica.

La delimitación del objeto aquí enumerado proviene de la protección de los datos personales. Hay varios aspectos que tradicionalmente ponen en crisis la intimidad y privacidad, pero se entiende que en la sociedad de la información el tratamiento de datos de las personas es el factor principal que pone en riesgo tales derechos. Es a través de estos datos que se materializan, almacenan y eternizan las informaciones sobre acciones privadas e íntimas de las personas, exigiendo una protección efectiva que limite el acceso indebido.

Para Bioni (2019, p. 57), no se trata solo de datos o de una base de datos, sino necesariamente de la dinámica de un sistema de información, que es lo que permite que una gran cantidad de hechos –datos– estén estructurados, organizados y gestionados para producir conocimientos que puedan revertirse para una toma de decisión; por ejemplo, una acción publicitaria. La tecnología de la información, desde los *bits* hasta los sistemas de información, ha permitido agregar y acumular datos que revelan una profusa información sobre las personas.

Sobre los sistemas jurídicos de protección de datos personales, Villegas Carrasquilla (2012) identifica tres visiones: el sistema de los Estados Unidos, el europeo, y el latinoamericano. Para el citado autor, el sistema de los Estados Unidos responde al problema de la privacidad –principalmente– mediante mecanismos de autorregulación; no obstante, está parcialmente protegida la privacidad por la cuarta enmienda de la Constitución (p. 128). En cambio, el modelo europeo está fundamentado a partir del artículo 8° del Convenio Europeo de Derechos Humanos de 1950 que garantiza el respeto a los derechos a la vida privada y familiar, como un derecho fundamental (p. 129). Por último, el modelo latinoamericano, es el que se ha basado principalmente en el derecho fundamental del habeas data, inclinándose posteriormente hacia un modelo de protección influenciado fuertemente por el de la Directiva Europea de 1995 (pp. 129-130).

Sostiene Villegas Carrasquilla (2012) que las principales diferencias entre los modelos europeo y estadounidense, se encuentran, que en este último, el concepto de libertad es la respuesta a la intromisión del Estado en la vida de los individuos, estando dirigido por ello hacia la autorregulación y las regulaciones sectoriales; en cambio, el enfoque europeo se manifiesta como una protección más general y uniforme, partiendo del concepto del derecho fundamental a la intimidad, en la cual el Estado debe intervenir activamente para proteger al individuo (p. 130).

Según Villegas Carrasquilla (2012, pp. 130-131), el sistema de protección de datos en América Latina tiene, en general, una característica particular que lo diferencia de los modelos europeo y estadounidense: el carácter constitucional de esta protección en una gran cantidad de países y sistemas jurídicos.

En las últimas décadas, las naciones han tratado de crear sistemas jurídicos para la protección de datos personales basados en leyes sectoriales y generales, pero la experiencia aún no ha arrojado resultados alentadores. Por esta razón, más recientemente, especialmente después de la creación del Reglamento General de Protección de Datos Personales de la Unión Europea - RGPD, las

ediciones y actualizaciones de las leyes de protección de datos se han convertido en el objeto de mayor preocupación en todos los continentes.

Esta investigación parte del estudio de las normas constitucionales e infraconstitucionales existentes, argentinas y brasileñas, sobre intimidad y privacidad, protección de datos personales y derecho sucesorio. Estos estándares van desde disposiciones genéricas hasta regulaciones específicas como las relaciones con los consumidores, el acceso a la información pública, la propiedad intelectual, las comunicaciones y el uso de Internet.

Los intentos iniciales de estandarizar el tema resultaron ineficaces debido a la dificultad de legislar sobre algo que no se limite a las fronteras territoriales de un país. Otros factores que debilitaron las primeras normas fueron la violación de derechos fundamentales y la sobrevaloración de la autonomía de la voluntad de los individuos.

Actualmente, debido al reconocimiento de que el tratamiento de datos personales es un asunto transnacional y que no permite una limitación excesiva, las naciones buscan en sus nuevas reglas adaptarse a un escenario internacional. En este panel, Argentina y Brasil fueron elegidos como objetivos de esta investigación, ya que, hasta ahora, hipotéticamente, cuentan con sistemas de protección de datos personales que no protegen adecuadamente la intimidad y privacidad del fallecido. Las dos naciones han intentado adaptarse al escenario internacional de protección de datos personales, pero se encuentran en realidades distintas.

Por caso, Brasil cuenta con una moderna Ley General de Protección de Datos Personales, fuertemente inspirada en el sistema europeo, y la Argentina aplica una ley vigente desde hace dos décadas; no obstante, aunque existen en esta Nación proyectos de ley mínimamente adecuados a los estándares internacionales, hasta la conclusión de este trabajo, no logró avanzar en los respectivos procesos legislativos.

Becerra y Garziglia (2019, párr. 3) precisan que la Argentina cerró la segunda década del siglo XXI con una ley de datos personales desactualizada y manoseada, pues pertenece a una edad antigua de internet. La Ley 25.326 fue

sancionada en el 2000 y sufrió al menos 85 modificaciones (vía decretos y resoluciones) que desdibujaron su objetivo, habilitando su incumplimiento por parte de los poderes del Estado. Este cuadro contrasta con los esfuerzos realizados en otras latitudes que concretaron cambios regulatorios recientes, como sucediera en la Unión Europea.

La investigación dirigida especialmente a la intimidad y privacidad de las personas fallecidas en Argentina y Brasil se realiza para garantizar la originalidad que requiere un trabajo de doctorado. La condición sin precedentes está garantizada por las raras producciones científicas que tratan el tema en uno o en otro país. Además, los trabajos encontrados y que sustentan esta tesis tratan temas aproximados, involucrando, en la mayoría de los casos, enfoques más generales, centrados en los derechos de la personalidad. Otro punto que vale la pena mencionar es que no se ha encontrado ningún trabajo que analice conjuntamente los sistemas jurídicos de ambos países.

El punto de partida se da entonces en un momento en que lo que se encuentra en Argentina y Brasil, son escasas y genéricas conclusiones doctrinales y científicas, normativas legislativas incompletas y ausencia de jurisprudencia, sobre el reflejo de la protección de datos personales en intimidad y privacidad *post mortem*. Un ejemplo de investigación que se acerca al objeto de esta tesis es el artículo de Jorge Luis Ordelin Font y Salete Oro Boff, publicado en 2019, titulado “La disposición *post mortem* de los bienes digitales: especial referencia a su regulación en América Latina”.

El trabajo mencionado se ocupa de varios derechos de la personalidad, tratados como bienes digitales, y analiza una visión general de América Latina en comparación con América del Norte y Europa. Font y Boff (2019, p. 56) concluyeron que la regulación jurídica de la disposición *post mortem* de los bienes digitales es necesaria en la actualidad, dada la importancia que adquiere el ámbito digital en las sociedades contemporáneas, en especial en el contexto latinoamericano. [...] Por ello, es necesario el establecimiento de regulaciones claras que precisen el poder de disposición sobre los bienes digitales posteriores al fallecimiento del titular, sean estos de carácter personal o no personal.

Con la idea del trabajo de Font y Boff, se busca en el Derecho europeo, especialmente el español y francés, bases legales capaces de ayudar a una futura propuesta regulatoria específica en Argentina y Brasil, para la protección de datos personales relacionados con la intimidad y privacidad del difunto. España y Francia cuentan con normas al respecto, que sirven como paradigmas para el tratamiento de datos de personas fallecidas y que garantizan, en cierta medida, la protección de la intimidad y privacidad después de la muerte.

En el ámbito judicial, según ya se ha dicho, no existe un tratamiento exhaustivo del tema en los principales tribunales de Argentina y Brasil, lo que se justifica por la aún escasa judicialización de situaciones relacionadas con la protección de datos personales. En efecto, se realizan algunos esfuerzos para encontrar en las decisiones que tratan los derechos de la vida íntima y privada, de la imagen, del honor, del olvido y de otros derechos de la personalidad, necesarios para un tratamiento eficaz de los datos personales, capaces de garantizar la inviolabilidad de la intimidad y privacidad *post mortem*.

Con ello, se traza el contexto en el que se inicia esta tesis, lo que hace que la investigación sea innovadora y con la expectativa de resultados y soluciones que puedan ayudar en la adecuación de los sistemas argentino y brasileño de protección de datos personales al vacío aquí presentado. El panorama que se muestra en este trabajo evidencia la magnitud de la importancia que los medios tecnológicos han ido adquiriendo en la vida humana, dejando claro que la estandarización de las realidades tecnológicas es cada vez más necesaria.

Capitulo II: La protección de los datos personales en Argentina y Brasil

1 Introducción

Este capítulo presenta los principales mecanismos jurídicos existentes en Argentina y Brasil para la protección de datos personales. Estos mecanismos –normas constitucionales e infraconstitucionales y jurisprudencia de los más altos tribunales– conforman los sistemas jurídicos que actualmente regulan la materia en ambos países. Son estos sistemas los que serán confrontados al final de este trabajo, con el fin de identificar si son capaces de garantizar la privacidad y la intimidad de las personas fallecidas.

Inicialmente se hace un acercamiento a la legislación argentina –en sentido amplio– de protección de datos personales, presentando las normas generales y especiales vigentes en el país. En este contexto, también da cuenta de los instrumentos jurídicos internacionales de los que la nación es signataria y la existencia de proyectos de ley relacionados con el tema.

También en un sentido amplio, la legislación brasileña de protección de datos personales se incluye en este capítulo. Con la presentación de estas normas es posible analizar y comparar conjuntamente los sistemas jurídicos que existen actualmente en Argentina y Brasil. La idea es demostrar la importancia que las dos naciones le han dado a temas como la protección de datos personales y, en consecuencia, la garantía de intimidad y privacidad en el panorama actual de revolución tecnológica.

Finalmente, este capítulo trae una búsqueda a las bases de datos de los principales tribunales de Argentina y Brasil. En este punto, algunas decisiones y resultados de búsqueda brindan una perspectiva real de cómo el tema de la protección de datos personales ha sido enfrentado por los poderes judiciales de dichas naciones.

2 La legislación argentina sobre la protección de los datos personales

Tarde, a fines de 2016, Argentina comenzó a discutir la necesidad de actualizar su legislación sobre la protección de datos personales. Al igual que Brasil, ambos países no acompañaron legislativamente la evolución operada en el campo tecnológico.

La Ley de Protección de Datos Personales actualmente se encuentra atravesando un proceso que tiene por objeto su reforma, la que comenzara en el 2016. A estos fines y en el marco del Proyecto denominado Justicia 2020, creado por el Ministerio de Justicia y Derechos Humanos, durante el año 2016 se recibieron aportes de los más diversos y prestigiosos representantes de todos los sectores de la sociedad civil (sector privado, gobierno, academia, tercer sector) respecto de los puntos a reformar de la norma, a partir de los cuales se elaboró el documento “Ley de Protección de Datos Personales en Argentina. Sugerencias y aportes recibidos en el proceso de reflexión sobre la necesidad de su reforma. Agosto-Diciembre 2016”, de la entonces Dirección Nacional de Protección de Datos, ahora denominada Agencia de Acceso a la Información Pública. (Faliero, 2018, p. 57).

En este sentido, el Poder Ejecutivo argentino durante el gobierno de Mauricio Macri tuvo la intención de derogar la Ley 25.326 de Protección de los Datos Personales y sus modificaciones introducidas por las leyes 26.343 y 26.951. Hasta la conclusión de este trabajo, algunos proyectos de ley que buscan actualizar la temática aún se encuentran en análisis por parte del Congreso Nacional argentino.

Sin embargo, la demora en completar los procesos legislativos aún mantiene la obsoleta norma de Protección de Datos los Personales vigente en el país. Antes de que se hagan comentarios sobre los proyectos de ley que se tramitan en el citado Congreso, y sobre la propia Ley de Protección de los Datos Personales, es necesario analizar la evolución legislativa argentina en la materia, a partir de su Constitución Nacional.

El estudio sobre la regulación legal de la protección de los datos personales en la Argentina, comienza con la Constitución originaria de 1853, reformada en 1994, que lo trata directa o indirectamente en los artículos 18, 19, 33, 42 y 43.

En términos generales, el artículo 18 prohíbe la violación de información personal, al afirmar que es inviolable la correspondencia epistolar y los papeles privados.

Sobre esta norma dice Iglesias (2011):

> [P]arece claro que todo dato que permite acceder al contenido de una comunicación, debe ser protegido dentro de la letra del artículo 18 de la constitución nacional, con prescindencia del soporte utilizado para su conservación, difusión o archivo. Debe tenerse en cuenta que, si bien algunos de estos documentos solo reflejan en forma parcial la correspondencia, otros, como los logs generados por programas de mensajería guardan el historial completo de las comunicaciones realizadas entre dos sujetos. De sostener la falta de necesidad de orden judicial previa sería permitir la existencia de una forma elíptica de limitar la privacidad de los sujetos de derecho, incompatible con los principios establecidos en la parte dogmática de nuestra norma fundamental. (párr. 10).

Cabe señalar que, aunque no existe lógicamente una disposición expresa en la norma constitucional argentina de 1853 sobre la protección de los datos personales transmitidos por medios virtuales, el artículo en cuestión protege este tipo de datos a través de una interpretación expansiva de su texto; sumándose a ello, en una visión de conjunto, los derechos implícitos o derechos no enumerados, introducidos en la reforma constitucional de 1860, especialmente en el artículo 33. Este artículo establece que las declaraciones, derechos y garantías que enumera la Constitución, no serán entendidos como negación de otros derechos y garantías no enumerados; pero que nacen del principio de la soberanía del pueblo y de la forma republicana de gobierno.

Resulta de vital importancia en la materia, comprender que, en la segunda mitad del siglo XIX, la protección al transporte de contenidos privados -propia del correo- fue asimilada por la telegrafía, y luego por la telefonía. El contenido transportado al ser privado, estaba protegido por la Constitución Nacional, que

establece en su texto, la inviolabilidad de la correspondencia epistolar y los papeles privados (artículo 18).

Refuerza Iglesias (2011, párr. 2), en consonancia con lo expuesto, que, aunque el artículo constitucional plantea una protección expresa sobre la correspondencia epistolar, es pacifica la jurisprudencia en considerar que las mismas se extienden a cualquier forma de comunicación con prescindencia del soporte utilizado.

Así también**,** el artículo 19 de la Constitución de la Nación Argentina, establece que las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados. Adviértase, que el texto constitucional extiende la protección prevista en el artículo 18 a toda conducta íntima. En efecto, a través de estos dispositivos la protección de la privacidad e intimidad está garantizada a nivel constitucional.

Según Maurino (2008, p. 8), el contenido mínimo que se le ha asignado a la tutela del artículo 19 se asocia con el resguardo de un ámbito material de privacidad, intimidad y vida personal y familiar.

Maurino (2008) sostiene:

> [L]os antecedentes constitucionales argentinos contienen una rareza en latinoamérica: un compromiso inequívocamente liberal con la garantía de un ámbito de soberanía exclusiva para el individuo, exento de la injerencia social y estatal: la garantía constitucional de la libre determinación de los individuos en su vida personal, consagrado definitivamente en el artículo 19 CN. Allí reside uno de los núcleos centrales de la autonomía individual. (p. 5).

El autor citado concluye:

> [E]sta dimensión sustantiva de la privacidad la asocia con el libre desarrollo de la personalidad, con las acciones que involucran cuestiones de moral individual, no social o intersubjetiva, con la libertad de los individuos para elegir y perseguir los planes de vida y los ideales de moral o de virtud personal sin interferencias externas; en particular, sin que el estado

> obligue, prohíba o condicione tales elecciones, o las acciones que los llevan a cabo. (p. 9).

El artículo 19 de la Constitución Argentina incluye parámetros generales que, interpretados de manera expansiva, garantizan la intimidad y privacidad de los usuarios de Internet, protegiendo sus acciones íntimas y privadas en el mundo virtual.

Producto de su reforma, en 1994, el texto constitucional refiere a la protección de los datos personales en particular, en escasos artículos, extendiéndose la misma, a los tratados incorporados en el artículo 75, inciso 22; resultando necesario, para una mejor comprensión de la temática en curso, del conocimiento de la jurisprudencia y la doctrina en la materia.

En relación al artículo 42 de la norma constitucional, dirigido específicamente a los consumidores y usuarios de bienes y servicios, se advierte que la protección de los datos personales no se encuentra expresamente señalada en el texto, si bien, a partir de su lectura, es posible extraer que los consumidores y usuarios tienen derecho a la protección de sus intereses económicos, a condiciones de trato equitativas y dignas, y a procedimientos efectivos para la prevención y solución de conflictos.

Sobre el dispositivo constitucional en foco**,** Ferrer de Fernández (2014) explica:

> [E]n el artículo 42 de la Constitución Nacional subyace la idea de mercado y de sistema democrático, por ejemplo, cuando se hace referencia al control de monopolios y a la defensa de la competencia. Ello sin embargo, no significa que en ese mercado signado por la libertad y la competencia no haya intervención del estado en la relación del consumo, muy por el contrario si la hay, y ello surge de los parágrafos segundo, en cuanto se establece que las autoridades proveerán a la protección de los derechos que se enumeran en el artículo, y tercero, en cuanto impone a la legislación establecer procedimientos eficaces para la prevención y solución de conflictos, y los marcos regulatorios de los servicios públicos de competencia nacional. (p. 1).

Se enfatiza que los datos personales agrupados de los consumidores y usuarios de bienes y servicios son los de mayor valor económico, ya que están estrechamente vinculados a la oferta en el mercado de consumo y al perfil del destinatario de la oferta; siendo necesario, profundizar en la protección de sus derechos. Precisamente por eso los datos personales de esta clase de ciudadanos reclaman la protección garantizada por el artículo 42 citado.

A diferencia de la redacción de los artículos de la citada Constitución estudiados hasta ahora, la siguiente disposición constitucional se refiere expresamente al derecho a la protección de datos personales mediante la existencia de la acción de hábeas data. A este respecto, el artículo 43, párrafo 3°, señala:

> Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística.

La protección de datos personales en Argentina necesitaba de un marco legal, que llegó en octubre de 2000, cuando se aprobó la Ley 25.326 de Protección de Datos Personales, el que se abordará a continuación. Al llamar al instituto una protección judicial de la privacidad, Ribeiro (2015) conceptualiza el *habeas data* en los siguientes términos:

> [U]na garantía fundamental que no se restringe a la proclamación de la protección de la privacidad de las personas, sino sirve también, como medio judicial específico para alejar la amenaza o daños en la vida íntima derivados de la recolección, almacenamiento, transmisión de datos sobre el sujeto, por agentes públicos o privados. (p. 27).

Las disposiciones normativas descritas brindan las bases constitucionales para la protección de los datos personales argentinos, que se demostrarán y estudiarán a la luz de las normas infraconstitucionales.

No obstante, aún en el marco constitucional, es importante mencionar a la Convención Americana sobre Derechos Humanos, máxime por estar incorporada al artículo 75, inciso 22, de la Constitución Argentina; tratado -que al igual que los allí mencionados-, en las condiciones de su vigencia, tiene jerarquía constitucional, no deroga artículo alguno de la primera parte de la Constitución y debe entenderse complementario de los derechos y garantías por ella reconocidos.

En tal sentido**,** Bidart Campos (1995, p. 590) advierte que, si a través del sistema de la integración regional se insertara un tratado de derechos humanos, nada obstaría a que este último alcance la jerarquía constitucional. Por caso, Argentina aprobó (01/03) y promulgó (19/03) en 1984 (Ley 23.054) la Convención Americana sobre Derechos Humanos (CADH), conocida como Pacto de San José de Costa Rica (PSJCR); incorporándose diez años después al texto constitucional.

La presentación oficial del Gobierno argentino de la CADH, realizada a través de la Secretaría de Derechos Humanos y Pluralismo Cultural del Ministerio de Justicia y Derechos Humanos, es la siguiente:

> Se trata de declaraciones, pactos, convenciones y protocolos incorporados en el artículo 75, inciso 22, de la Constitución, en la reforma de 1994, o cuya jerarquía constitucional fue otorgada por leyes posteriores, y deben entenderse como complemento de los derechos y garantías en ella reconocidos (Argentina, 2016, p.6).

Esta norma incluye en el artículo 11, párrafos 2° y 3°, disposiciones que, además de las extraídas del texto constitucional**,** y mencionadas anteriormente, también generalmente garantizan la protección de datos en Argentina. El párrafo 2° dice que nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación; estableciendo el párrafo 3°, que toda persona tiene derecho a la protección de la ley contra esas intrusiones o esos ataques. La gran influencia de esta norma es notable en las disposiciones constitucionales estudiadas hasta ahora, especialmente las contenidas en los artículos 18, 19, 33, 42 y 43 de la Constitución Argentina.

Al comentar sobre la privacidad a la luz de la CADH, Petrino (2013) explica que de acuerdo con una amplia doctrina:

> [L]a privacidad abarcaría las acciones (efecto de hacer) a través de las cuales las personas ejercen libremente su autonomía sobre cuestiones significativas, aún aquellas que se realicen a la luz del día y con amplio conocimiento público, porque se exteriorizan al público, comprendiendo no solo la esfera doméstica, el círculo familiar y de amistad, sino laboral y social. (p. 211).

Obviamente, la protección de la privacidad va más allá de la idea de actuar exclusivamente en un entorno privado, extendiéndose a cualquier otro entorno, incluido el entorno virtual y, en consecuencia, a los datos personales generados allí. De ahí la legitimidad de la aplicación del PSJCR al sistema legal argentino de protección de datos.

Aún en el ámbito de los estándares internacionales, Argentina se convirtió, con la publicación de la Ley 27.483 (01/02/2019), en signataria del Convenio de Estrasburgo, Francia. Esta norma, que se denominó "Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal", surgió el 28 de enero de 1981. Aun siendo antiguo, el Convenio Internacional tiene una amplia aplicación en la actualidad, principalmente en la regulación del carácter transnacional de los datos personales. En este sentido, según el considerando 4 es reconocida la necesidad de conciliar los valores fundamentales del respeto a la vida privada y de la libre circulación de la información entre los pueblos.

En lo que respecta a la regulación central en la protección de los datos personales, el Convenio 108 de 1981 o Convenio de Estrasburgo fue el primer cuerpo sistematizado regional e internacional en el que se trató específicamente la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, sustentado en el derecho a la privacidad, del cual se derivaron las directivas y los reglamentos (Faliero, 2018, p. 58).

El Convenio de Estrasburgo fue actualizado el 8 de noviembre de 2001, mediante un protocolo adicional diseñado para adaptar la norma a la realidad tecnológica, que tuvo en cuenta la importancia del flujo de información entre los

pueblos y que, con la intensificación de los intercambios de datos de carácter personal a través de las fronteras nacionales, se hizo necesario garantizar la protección efectiva de los derechos humanos y de las libertades fundamentales y, en particular, del derecho al respeto de la vida privada, en relación con tales intercambios.

Vale decir aquí que ninguna de las disposiciones de esta norma menciona la protección de datos de las personas fallecidas. Varias de las disposiciones previstas en el Convenio de Estrasburgo, por ejemplo, las definiciones y los derechos de información, finalidad y oposición, que se estudiarán más adelante, ya habían sido incorporados a la legislación argentina por la Ley de Protección de los Datos Personales. Aun así, la norma sigue siendo de fundamental importancia para que el país se adapte mínimamente a los sistemas internacionales de transferencia de datos.

En la visión de Palomo, Piccardi y Guillet (2020, p. 207) la Ley de Datos Personales 25.326 y el Convenio de Estrasburgo para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de carácter Personal, es un muy buen marco para a partir de allí, ampliar los alcances, en línea con el Reglamento General de Protección de Datos (RGPD) de la Unión Europea y demás instrumentos legales internacionales.

Este estudio de la regulación infraconstitucional argentina sobre protección de datos se inicia con el Decreto-Ley 20.216, “Ley de Correos”, que, aunque fue publicado el 23 de marzo de 1973, ha sufrido cambios posteriores y, por lo tanto, es efectiva hoy a la garantía constitucional sobre la inviolabilidad de la correspondencia y los papeles privados, y su debido resguardo, potencialmente en peligro por la conducción de aquéllos por terceros.

Esta norma refleja el monopolio estatal sobre el transporte de comunicaciones escritas en Argentina, que se establece expresamente en el artículo 2°, que queda exclusivamente reservado al Estado la admisión, transporte y entrega de las comunicaciones escritas, grabadas o realizadas por cualquier otro procedimiento asimilable que se encuentren cerradas, y las abiertas que tengan carácter actual y personal y todo sobre o pliego cerrado provisto de dirección.

Así también, el decreto-ley prescribe en su título III (De la inviolabilidad y del secreto postal), que “La inviolabilidad de los envíos postales, importa la obligación de no abrirlos, apoderarse de ellos, suprimirlos, dañarlos o desviarlos intencionalmente de su curso, ni tratar de conocer su contenido, así como de no hacer trascender quienes mantienen relaciones entre sí o dar ocasión para que otros cometan tales infracciones”. En orden a ello, “Todo empleado o persona afectada al servicio, está obligada a prestar juramento de guardar estrictamente el secreto postal” (artículo 6º).

No obstante, lo expuesto, se aclara, que el Decreto 151 (18/01/74), reglamentario de la Ley de Correos, determina, que “El Estado ejerce el monopolio postal a través de la Administración de Correos. No están incluidos en el monopolio postal los libros, impresos, muestras, las cartas y tarjetas postales que hayan cumplido su fin primitivo, las piezas de procedimientos judiciales y otros envíos similares a los enunciados en este párrafo, a condición, en todos los casos, de que circulen abiertos y no tengan carácter actual y personal. a) Se considera comunicación de carácter actual la de reciente data o que tiene vigencia para ambos corresponsales. Cualquiera fuere el caso dejará de ser actual una vez entregada al destinatario o a quien correspondiere. b) Se considera comunicación personal a la que tiene ese carácter específico y a toda aquella, manuscrita o impresa, cualquiera fuere su texto, que ostente el nombre de la persona a que está dirigida y lleve la firma, de puño y letra o autografiada, del remitente o de persona autorizada o que lo represente. c) Los reglamentos determinarán los requisitos que deben reunir los envíos para ser considerados cerrados” (artículo 2°).

El Decreto-Ley 20.216/73, en algunos aspectos, va a contramarcha de lo que sucede con la información y las comunicaciones en Internet. Por ejemplo, la Ley de Correos prohíbe la expedición y circulación por las oficinas de correos, de cualquier tipo de escrito, ilustración y objetos de carácter inmoral o delictuoso (artículo 23), como así también, “[…] la expedición y circulación por las oficinas de correos de todo tipo de correspondencia, objetos y/o literatura impresa manuscrita o grabada, cuya finalidad sea la difusión de ideologías, doctrinas o sistemas

políticos, económicos o sociales, tendientes a derogar la forma republicana y representativa de gobierno. La prohibición alcanzará también a esos mismos envíos, cuando atenten contra la seguridad pública o privada, o los intereses del estado, las modalidades de vida democrática previstas en la Constitución Nacional, los principios morales y el respeto a la persona humana […]" (artículo 24).

Este monopolio permitió al Estado tener un dominio parcial y cuestionable sobre el contenido de las comunicaciones transmitidas por el Correo Argentino, que se explica en los artículos 25 y 27 de la ley en cuestión.

De acuerdo con el citado artículo 25:

> [S]e prohíbe escribir o incluir comunicaciones de carácter actual y personal en las encomiendas y demás envíos postales que no estén destinados por la reglamentación al intercambio de comunicaciones de ese carácter, así como incluir en las piezas de correspondencia sujetas a una tasa menor, envíos que tengan fijada una tasa mayor, salvo que se encuentren franqueados en las condiciones que determine la reglamentación.

En relación al artículo 27:

> [C]uando la autoridad postal presumiera la existencia de elementos de circulación prohibida en envíos postales cerrados, podrá realizar la apertura con el consentimiento y presencia del impositor o destinatario o a su inmediata devolución en caso de negativa. Si del procedimiento surgiera la evidencia de tales elementos, se ajustará su contenido conforme a esta ley y a lo dispuesto en la reglamentación.

Pero el monopolio estatal argentino sobre el transporte postal ha perdido fuerza a lo largo de los años. En 1993, el Decreto 1187, que abordó el Régimen Postal, Registro Nacional de Prestadores de Servicios Postales, Publicidad del Servicio y Responsabilidad Frente al Cliente, entre otras disposiciones, tornó abierto y competitivo el mercado postal local e internacional en Argentina. Una de las principales justificaciones está en los considerandos del Decreto en foco que advirtió:

> [Q]ue ya el Decreto N° 1842/87 había establecido un régimen de desmonopolización de los servicios públicos prestados por las empresas estatales, manifestando en sus considerandos que el mantenimiento de monopolios estatales en el área de los servicios y bienes destinados al público, ha perdido todo sustento fáctico, puesto que obra en detrimento del bienestar público y del desarrollo económico, tecnológico y social de la Nación (Considerando 3).

Con la revolución tecnológica, los servicios postales en todo el mundo comenzaron a enfrentar una crisis importante, teniendo que adaptarse a la nueva sociedad informatizada. Las comunicaciones pasaron a escribirse y realizarse principalmente en el entorno virtual, lo que hace que estos servicios necesiten buscar alternativas para su mantenimiento. Reglas como las de la Ley de Correos, que durante un tiempo considerable han servido de base legal para la protección de las comunicaciones, comienzan a caer en desuso y, cuando se invocan, deben interpretarse ampliamente para adaptarse a la realidad.

Otra de las leyes argentinas de importancia, que también garantiza la protección de datos, es la Ley de Propiedad Intelectual 11.723. Publicada el 30 de septiembre de 1933, aún protege ampliamente la imagen de las personas, incluidas las fallecidas, lo cual es de interés para este estudio; explorándose a continuación. El artículo 31 de la Ley 11.723, más allá de las particularidades del caso, que exige distinguir entre imagen y retrato –como más adelante se explicará–, dispone:

> [E]l retrato fotográfico de una persona no puede ser puesto en el comercio sin el consentimiento expreso de la persona misma y muerta ésta, de su cónyuge, hijos o descendientes directos de éstos, o en su defecto, del padre o de la madre. Faltando el cónyuge, los hijos, el padre o la madre, o los descendientes directos de los hijos, la publicación es libre.
> La persona que haya dado su consentimiento puede revocarlo resarciendo daños y perjuicios.
> Es libre la publicación del retrato cuando se relacione con fines científicos, didácticos y en general culturales, o con hechos o acontecimientos de interés público o que se hubieran desarrollado en público.

Porcelli (2017) ilustra la oportunidad de la aplicación de este artículo en la actualidad:

> [U]n tema muy interesante lo constituyen las selfies, su intercambio se encuentra en crecimiento vía redes sociales como *Facebook* e *Instagram*. Frente a este hecho social, que recién comienza, la selfie obtiene protección legal en el artículo 31 de la Ley N° 11.723 que establece que el retrato fotográfico de una persona se encuentra bajo su órbita de control y no puede ser utilizado sin su consentimiento. (p. 2437).

Sobre la aplicación de esta norma, Iglesias (2015, p. 140) explica que la interpretación del artículo 31 de la Ley 11.723 debe ser necesariamente restrictiva en cuanto a la amplitud de las autorizaciones dadas. En consecuencia, se prohíbe el uso de cualquier consentimiento que no sea el sujeto de la autorización.

La preocupación del autor está estrechamente relacionada con el uso ilimitado de imágenes y otros datos personales, de los usuarios de Internet por parte de los motores de búsqueda y las redes sociales que utilizan sus complejos "términos y condiciones de uso", aceptados a menudo sin una lectura adecuada para disponer libremente de las imágenes y datos personales de los solicitantes de registro.

Ello por cuanto para que tenga acceso a los diversos servicios ofrecidos en Internet, el usuario necesita estar de acuerdo con las políticas de privacidad y los términos de uso asociados a estos servicios. Lo que ocurre es que los usuarios, en la gran mayoría de los casos, no saben exactamente lo que están consintiendo, ya que los documentos son muy largos y la mayoría no los lee. Consecuentemente, a partir del análisis de los términos de uso y políticas de privacidad de estos servicios, se percibe que los usuarios están delegando en los proveedores el acceso indiscriminado a sus informaciones personales (Silva, 2015, p. 15).

Más allá de estas consideraciones, resulta oportuno destacar sobre el derecho a la imagen, que “En la ley 11.723 se encuentran varias normas (arts. 31, 33 y 35) referidas a una cuestión que escapa a la naturaleza de nuestra materia: el derecho de la persona retratada sobre su imagen, porque a diferencia del retrato,

la imagen personal no es una obra aunque su custodia se encuentre regulada dentro de la ley 11.723; como otros derechos de la personalidad general –o derechos personalísimos– corresponde que sea legislada en el Código Civil" (Villalba y Lipszyc, 2001, p. 42); como sucede en la actualidad con el Código Civil y Comercial de la Nación.

El artículo 34 de la Ley 11.723 en cambio, hace referencia al derecho de propiedad sobre la obra fotográfica. Según la disposición legal en cuestión, es de 20 años, desde la primera publicación.

Con relación a la imagen, es dable observar su evolución en las redes sociales. Estos mecanismos de interacción social utilizan contratos electrónicos complejos para hacer que sus usuarios renuncien a los derechos sobre sus imágenes. Por lo tanto, es de suma importancia comparar estos contratos con la legislación ahora comentada.

Dice Dorado (2016):

> [E]l proceso de registro o suscripción a una red social presupone la aceptación de un instrumento jurídico complejo -pues suele estar formado por varios cuerpos escritos, entre los que se incluyen las "Política de Privacidad", los "Principios", las "Normas de Publicidad" y "de la Plataforma", las "Políticas de Cookies", las "Políticas de Propiedad Intelectual" o "Políticas de Copyright", las "Directrices de Fotos", "Directrices Comunitarias", entre otros nombres que cada red social les otorga-, que se conoce como "Términos o Condiciones de Uso", los cuales son imprescindibles para dejar constancia de la mecánica de su funcionamiento, además de regular los derechos y las obligaciones de los usuarios y del prestador del servicio de red social. (p. 1).

Complementando las disposiciones de los artículos 31 y 34 de la Ley de Propiedad Intelectual de Argentina, se encuentra el artículo 35, que establece que, "El consentimiento a que se refiere el artículo 31 para la publicación del retrato no es necesario después de transcurridos 20 años de la muerte de la persona retratada. Para la publicación de una carta, el consentimiento no es necesario después de transcurridos 20 años de la muerte del autor de la carta. Esto aún en

el caso de que la carta sea objeto de protección como obra, en virtud de la presente Ley".

Debe aclararse, siguiendo a Lipszyc (1993, p. 61), que "El objeto de la protección del derecho de autor es la obra. Para el derecho de autor, *obra* es la expresión personal de la inteligencia que desarrolla un pensamiento que se manifiesta bajo una forma perceptible, tiene originalidad o individualidad suficiente, y es apta para ser difunidda y reproducida".

Respecto de la fotografía, la Ley 11.723 (artículo 1°) dispone la protección de las mismas como obras, y resulta lógico que "las fotografías que presentan alguna originalidad en el encuadre o en la composición o en cualquier otro elemento importante de la imagen, sin lugar a dudas son acreedoras al igual que las demás obras artísticas, a la protección del derecho de autor". (Lipszyc, 1993, p. 84).

A diferencia de la fotografía –en los términos detallados precedentemente–, la imagen no tiene conceptualmente la protección como obra, de acuerdo a lo dispuesto por Ley de Propiedad Intelectual.

Por tal motivo, además del artículo 31 de la Ley 11.723, en la actualidad debemos remitirnos a las disposiciones contenidas en el artículo 53 del Código Civil y Comercial argentino.

En consecuencia, si nos atenemos a lo señalado en el artículo 31 citado, podremos observar que "reconoce el señorío absoluto de la persona retratada –y a su muerte, de determinados herederos– a autorizar la publicación de su retrato. Si bien sólo menciona el *retrato fotográfico*, en esta expresión están comprendidas todas las formas de fijación de la imagen, cualesquiera sea el modo de reproducción o de comunicación pública" (Villalba y Lipszyc, 2001, p. 43).

Los autores citados destacan lo resuelto en "W. de F., C.F. c. Ediarte S.A." (CNCiv., sala D, octubre 10-1996, E.D., 171-94), actuaciones en las cuales el tribunal sostuvo, que "La expresión poner en el comercio, usada en el art. 31 de la ley 11.723, debe entenderse en el sentido amplio de exhibición, difusión o publicación con cualquier finalidad (cf. Zavala de González, "Derecho a la intimidad", pág. 95)".

Villalba y Lipszyc (2001) con acertado criterio afirman, que aunque el artículo 31 de la Ley 11.723 no lo diga expresamente, “la persona tiene un derecho anterior a que no se fije su imagen sin autorización, aunque no se publique, ya que la fijación es por sí misma un acto de reproducción” (p. 43).

Los autores insisten en destacar, que “se trata de un derecho de la personalidad distinto del que surge de un acto de creación intelectual, y por lo tanto, no tiene la naturaleza propia de un derecho de autor” (p. 43).

Retomando la relación y las diferencias entre la Ley 11.723 y el CCyCN, Garsco (2015) advierte:

> [E]l artículo 53 in-fine del nuevo Código establece que pasado veinte años de la muerte de la persona, la publicación de su imagen es libre, en la medida que “no sea ofensiva”; asimismo, el artículo 35 de la ley 11.723, dispone que la publicación del retrato es libre luego de trascurrido veinte años de la muerte de la persona retratada.- No obstante, cabe tener en cuenta que el artículo 34 de la ley 11.723 dispone que el derecho de propiedad sobre la obra fotográfica, en cabeza del autor, es de veinte años a partir de la fecha de la primera publicación. Por lo tanto, puede ocurrir que la publicación de la imagen sea libre porque ha transcurrido el plazo previsto en el artículo 53 respecto a la protección del derecho personalísimo de la imagen en cabeza del retratado, pero que aún no haya transcurrido el plazo previsto en el artículo 34 de la ley 11.723, respecto al derecho de autor. (p. 6).

Otro estándar legal argentino importante relacionado con la protección de datos es la Ley 27.078, de Tecnologías de la Información y las Comunicaciones. Publicada el 16 de diciembre de 2014, conocida como Ley Argentina Digital, siendo su objeto, el interés público en el desarrollo de las Tecnologías de la Información y las Comunicaciones, las Telecomunicaciones, y sus recursos asociados, estableciendo y garantizando la completa neutralidad de las redes (artículo 1°).

Según Iturralde (2019):

> [L]a sanción de la Ley Argentina Digital apostó a la regulación de la infraestructura de transporte de comunicación, involucrando las redes telefónicas, de

> conexiones de banda ancha y de televisión por cable. Autorizó la convergencia y el triple play, permitiendo que las empresas telefónicas brinden servicios de comunicación audiovisual -exceptuando la televisión digital. (p. 66).

En este paso, modernizando el concepto de correspondencia introducido en la Ley Postal Argentina ya estudiada, el artículo 5° de la Ley Argentina Digital establece:

> Inviolabilidad de las comunicaciones. La correspondencia, entendida como toda comunicación que se efectúe por medio de Tecnologías de la Información y las Comunicaciones (TIC), entre las que se incluyen los tradicionales correos postales, el correo electrónico o cualquier otro mecanismo que induzca al usuario a presumir la privacidad del mismo y de los datos de tráfico asociados a ellos, realizadas a través de las redes y servicios de telecomunicaciones, es inviolable. Su interceptación, así como su posterior registro y análisis, sólo procederá a requerimiento de juez competente.

Con el advenimiento de este artículo, hay una actualización necesaria del concepto de correspondencia, hasta ahora regulado en la Ley Argentina solo por la Ley de Correos. La Ley Argentina Digital inserta expresamente la protección de la correspondencia electrónica y de la intimidad y privacidad virtuales en la legislación nacional argentina, teniendo en cuenta la necesidad de adaptar las normas a la tecnología y a la realidad actual.

No se puede negar el gran progreso realizado por la Ley Argentina Digital. La inserción en la legislación argentina de la protección de la intimidad-privacidad virtual, que hasta entonces era inexistente y significaba que la protección legal se buscaba de manera análoga, ni garantizando siempre la protección adecuada requerida en el texto constitucional.

En este contexto incluyo, el Código Civil y Comercial de la Nación (Ley 26.994; octubre de 2014), como uno de los marcos legislativos argentinos más importantes en la materia.

Según Becerra y Zárate (2015):

> [L]os aspectos regulatorios recientemente incorporados al Código Civil y Comercial (CCC) en virtud de la Ley Nº 26.994 (B.O. 31/10/2014), tal cual lo expresa la doctrina muestran como uno de sus mayores logros, el establecimiento de un régimen sistemático de los derechos de la personalidad, y creemos que en base a la interpretación de las clausulas abiertas que hará la doctrina y la jurisprudencia se logrará la protección plena de la persona humana frente al entorno tecnológico. (p. 217).

En relación a la protección de los datos personales, el nuevo código trajo varios dispositivos que pueden ser aplicados para garantizar directa o indirectamente la intimidad y privacidad virtuales. Becerra y Zárate (2015, p. 217) afirman que existe un amplio reconocimiento de los derechos personalísimos (artículos 51 y ss.) que incluye la inviolabilidad de la persona humana y establece que en cualquier circunstancia tiene derecho al reconocimiento y respeto de su dignidad.

Sobre el artículo 51 del Código Civil y Comercial de la Nación Argentina, explica Cánepa (2019):

> [A] partir de allí puede concluirse que la inviolabilidad de la persona humana y el reconocimiento de su dignidad constituyen la base sobre la que se sustenta todo el capítulo y en función de la cual deberá interpretarse el alcance de los demás derechos personalísimos, resultando los artículos siguientes una enunciación –meramente ejemplificativa- de sus diversas manifestaciones. (p. 42).

Complementando lo señalado, Becerra y Zárate (2015) sostienen:

> [E]l Nuevo Código extiende su tutela a los Derechos espirituales que se enuncia en el (artículo 52) la imagen, la intimidad, el honor, la reputación, así como cualquier otro que resulte una emanación de la dignidad personal y le dan a la persona la posibilidad de reclamar la prevención y la reparación del daño sufrido. (p. 217).

Según Cánepa (2019):

> [E]sta norma podría ser interpretada en el sentido de que se encuentra referida únicamente a los derechos

> que protegen la integridad espiritual (‘la intimidad personal o familiar, honra o reputación, imagen o identidad’ y a otras afecciones a la dignidad); o bien, con mayor amplitud, entendérsela como una norma de carácter genérico inclusiva de otras manifestaciones de los derechos personalísimos que exceden las expresamente mencionadas. (p. 45).

Esta declaración justifica la aplicación de las disposiciones legales aquí comentadas al objeto de este trabajo, especialmente en lo relacionado con la protección de la intimidad y privacidad en sus manifestaciones virtuales. El carácter generalista de la norma es propio de los códigos civiles, y es natural mencionar protecciones y garantías genéricas o implícitas. Por este motivo, no se mencionan expresamente protecciones relacionadas con datos personales, intimidad o privacidad virtuales en el texto codificado.

El artículo 53 del Código Civil y Comercial de Argentina, ya mencionado en este trabajo, trae la protección de la imagen (artículo 53) estableciendo que es necesario su consentimiento para captar o reproducir la imagen o la voz de una persona (Becerra y Zárate, 2015**,** p. 217).

Explica Cánepa (2019):

> [E]l artículo 53 del Código reproduce en esencia la redacción del artículo 31 de la Ley 11.723 de Propiedad Intelectual, aunque mejorando su redacción. Así, no se protege ya sólo la comercialización, sino también la captación y la reproducción; incluyendo el nuevo Código la protección de la voz, además de la imagen; a la vez que regula la protección *post mortem* de este derecho, permitiendo a la persona designar por disposición de última voluntad a quien podrá manifestar el consentimiento para la reproducción, pudiendo sus herederos prestarlo únicamente en el caso en que la persona fallecida no lo haya designado en tal forma. (p. 48).

De gran importancia para este trabajo, la disposición final del artículo 53 en cuestión puede indicar una posibilidad para el procesamiento de datos personales de personas fallecidas; así señala:

> En caso de personas fallecidas pueden prestar el consentimiento sus herederos o el designado por el

> causante en una disposición de última voluntad. Si hay desacuerdo entre herederos de un mismo grado, resuelve el juez. Pasados veinte años desde la muerte, la reproducción no ofensiva es libre.

El dispositivo legal en foco se ocupa de la protección de la imagen y la voz. No debe olvidarse que estas manifestaciones de la naturaleza humana hoy en día se convierten en datos y se almacenan en dispositivos y redes informáticas, que a menudo contienen información íntima y están relacionadas con la privacidad.

Por lo tanto, su aplicación a la protección de datos personales debe considerarse e interpretarse junto con leyes específicas, por caso, las leyes de Propiedad Intelectual y de Protección de los Datos Personales, analizadas a continuación.

Becerra y Zárate (2015), respecto a la prevención de la violación de la intimidad y privacidad virtuales y de los datos personales, expresan:

> [L]a responsabilidad civil es regulada como un sistema que admite tres funciones. Preventiva, resarcitoria y disuasiva. Es importante destacar que por primera vez se incorpora toda una sección destinada a la Prevención (Artículos 1710 a 1713). Esta faz preventiva es fundamental cuando tratamos las violaciones a la intimidad y privacidad por las consecuencias que acarrean en los entornos tecnológicos caracterizados por la multiplicación de las conductas dañosas que alcanzan cifras inimaginables tornando casi nulo el derecho al olvido. (pp. 222-223).

Por caso, el artículo 1770 del Código Civil y Comercial argentino dispone:

> Protección de la vida privada. El que arbitrariamente se entromete en la vida ajena y publica retratos, difunde correspondencia, mortifica a otros en sus costumbres o sentimientos, o perturba de cualquier modo su intimidad, debe ser obligado a cesar en tales actividades, si antes no cesaron, y a pagar una indemnización que debe fijar el juez, de acuerdo con las circunstancias. Además, a pedido del agraviado, puede ordenarse la publicación de la sentencia en un diario o periódico del lugar, si esta medida es procedente para una adecuada reparación.

De acuerdo con Lorenzetti (2015):

> [S]e provee, además, según lo normado por el artículo 1770, de una acción de cesación –y en su caso de indemnización– para supuestos de intromisión en la vida ajena a través de publicación de retratos, difusión de correspondencia, mortificación a sujetos en sus costumbres, sentimientos o perturbaciones de la intimidad a través de cualquier medio. [...] En estas previsiones detectamos también la enfática postura que asume el Código en relación con la preservación de la esfera individual de la persona al intentar sustraerla de invasiones provenientes tanto de particulares como del poder público. (p. 7)

Obsérvese que el sistema de responsabilidad civil extraído del Código Civil y Comercial de la Nación Argentina es una herramienta importante para combatir la violación de la intimidad, de la privacidad y de los datos personales. Aunque no hay una referencia expresa en el artículo que pueda vincular su uso en la responsabilidad civil de quienes violan los datos personales, es cierto que este dispositivo legal brindará la seguridad mínima para la sanción. Del mismo modo, su aplicación en casos de violación de datos personales, siendo aclarada por la jurisprudencia, también crea un mecanismo preventivo, de acuerdo a lo que explicaran anteriormente Becerra y Zárate.

En este ámbito de prevención y sanción, surge en el sistema legal argentino la Ley 26.388 de Delitos Informáticos (24/06/2008), que modificó el Código Penal argentino, insertando la responsabilidad penal por violar la intimidad-privacidad virtual y los datos personales. A lo largo de sus 15 artículos, la ley crea y modifica tipos penales, adaptando así la legalización criminal común a la evolución tecnológica y la inserción de tecnología en la vida cotidiana de las personas.

Según Riquert (2008):

> [H]a significado un sustancial avance sobre temas cuya consideración venía siendo reclamada desde mucho tiempo atrás, poniendo fin a antiguas discusiones jurisprudenciales y doctrinarias. A su vez, resulta un aporte hacia la armonización legislativa en la materia con otros países del bloque regional que se ocuparan antes de esta problemática en un modo más integral (p. 58).

En la misma dirección, Pilnik Erramouspe (2010) explica:

> [N]uestro país ha dado un gran paso al sancionar la ley 26.388 y, con ella, ha armonizado nuestra legislación con la de varios de los miembros regionales del Mercosur. Con esta nueva ley [añade] se podrán perseguir y penar muchas conductas que, ante el vacío legal, quedaban impunes y generaban cuantiosas pérdidas económicas. Aun así [reconoce el autor], todavía resta regular la situación de todos los actores que aparecen involucrados en la interacción electrónica, ya que es a partir de una correcta distinción de qué roles cumplen cada uno, que se podrán delimitar responsabilidades. (p.1234).

Entre las principales novedades traídas por la nueva ley penal, y de mayor interés para este trabajo, están las insertadas en los artículos 153, 155, 157 y 157 bis del Código Penal, las que serán brevemente analizadas a continuación. El artículo 153, que fue reemplazado por artículo 4° de la Ley 26.388, protege la inviolabilidad de la comunicación electrónica, carta, pliego cerrado, despacho telegráfico, telefónico o de otra naturaleza:

> [S]erá reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.
> En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.
> La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.
> Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena.

Está claro que el legislador estaba preocupado por adaptar la ley al uso creciente de la tecnología, extendiendo la protección de la intimidad y privacidad al

mundo virtual**;** asegurando así la criminalización de la violación de las comunicaciones electrónicas. También buscó castigar la publicación inadecuada de estas comunicaciones, penalizando a los infractores con una pena más alta y, en el caso de un funcionario público, también incluyó la consecuencia extrapenal de la descalificación por el ejercicio del servicio público.

De acuerdo con Turnes (2016, p. 41) de su lectura, se advierte, que el centro de la modificación estuvo orientado a incluir en forma clara y directa, las comunicaciones electrónicas, equiparándolas con las telefónicas y las cartas epistolares.

Aunque el artículo 155 del Código Penal argentino no prevé una sanción represiva de la libertad personal, dado que la sanción que se impondrá es solo una multa, tiene una disposición importante relacionada a la intimidad-privacidad de los datos personales, ya que el propósito es proteger la información privada contra la publicación no autorizada.

En la lección de Turnes (2016):

> [L]a introducción que se hizo al artículo, más relevante, fue el reemplazo de la fórmula “correspondencia” por “una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza”, volviéndose de este modo, absolutamente abarcativa de los diversos modos de comunicación modernos, al ampliar el objeto del delito. Al igual que en el artículo 153, la norma requiere que la publicación se produzca de forma indebida, sin derecho, circunstancia que fue debidamente analizada en su oportunidad. (p. 49).

Otra disposición legal importante para combatir la violación de datos personales es el artículo 157 del Código Penal, reemplazado por el artículo 7° de la Ley 26.388, que precisa que será reprimido con prisión de un mes a dos años e inhabilitación especial de uno a cuatro años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos. Dirigido a proteger los datos en poder del Estado y considerados secretos, este artículo protege indirectamente los datos personales y la información de los

ciudadanos, ya que, en múltiples casos, estos datos y la información están relacionados con la vida privada.

Finalmente, se observa el artículo 157 bis, que fue reemplazado por el artículo 8° de la Ley 26.388:

> [S]erá reprimido con la pena de prisión de un (1) mes a dos (2) años el que:
> 1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;
> 2. Ilegítimamente proporcionare o revelare a otra información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.
> 3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.
> Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años.

Una vez más, el derecho penal protege la privacidad y la intimidad, ya que castiga el acceso no autorizado a las bases de datos reservadas por cualquier persona, agravando la pena cuando se trata de un funcionario público. De acuerdo con Arocena (2012**,** p. 976), es indudable que todo acceso cognitivo no autorizado a un banco de datos reservado importa una lesión al derecho a la "intimidad" y a la "privacidad" de la persona física o de existencia ideal que es titular de los datos.

Continuando el estudio de la legislación argentina en materia de protección de datos, me remito a la Ley 27.275, del derecho de acceso a la información pública. A través de esta norma, la ley argentina se ha preocupado por disciplinar el tratamiento de la información pública y la información personal en poder del Estado. Explican Piana y Amosa (2018, p. 246) en el caso de la información pública, este derecho es un derecho humano, ciudadano y colectivo, basado en el derecho a petición y la obligación de transparencia de la actividad gubernamental, que tiene por principal obligado al Estado.

Sin embargo, el acceso a la información pública, por supuesto, no puede ser irrestricto y debe preservar la seguridad pública, el mantenimiento de datos personales, la intimidad y privacidad de los ciudadanos.

En cuanto al objeto de esta investigación, los artículos 8°, “i”, y 34, de la Ley de Acceso a la Información Pública incluyen las excepciones al acceso a la información pública, cuando se trata de datos personales, consagrando así la protección de la intimidad-privacidad.

El mencionado artículo 8º, “i”, precisa:

> [E]xcepciones. Los sujetos obligados sólo podrán exceptuarse de proveer la información cuando se configure alguno de los siguientes supuestos: (...) i) Información que contenga datos personales y no pueda brindarse aplicando procedimientos de disociación, salvo que se cumpla con las condiciones de licitud previstas en la ley 25.326 de protección de datos personales y sus modificatorias…

El Artículo 34, dispone:

> [E]xcepciones a la transparencia activa. A los fines del cumplimiento de lo previsto en el artículo 32 de la presente ley, serán de aplicación, en su caso, las excepciones al derecho de acceso a la información pública previstas en el artículo 8° de esta norma y, especialmente, la referida a la información que contenga datos personales.

Se nota que la ley argentina se ha preocupado por garantizar la publicidad adecuada de la información pública, sin permitir la violación de la intimidad y privacidad de las personas. En este contexto, la provisión de datos privados que sean propiedad del Estado, solo ocurre en situaciones excepcionales, y existe la obligación de respetar las disposiciones de la Ley 25.326 de protección de datos personales.

Además de las normas ya mencionadas, el sistema jurídico argentino de protección de datos personales también cuenta con la Ley 26.529, de derechos del paciente en su relación con los profesionales e instituciones de la salud (19/11/2009). Esta ley considera como derechos esenciales del paciente (artículo 2), entre otros, la intimidad y la confidencialidad.

Por lo tanto, cuando el caso requiera el tratamiento de datos personales, la Ley 26.529 debe ser interpretada en conjunto con la Ley de Protección de Datos

Personales. Es que, en tales situaciones, el artículo 8 de esta Ley crea la posibilidad de manejo de los datos de los pacientes estableciendo:

> [L]os establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional.

Si bien la Ley de Protección de Datos Personales tiene autorización para la recolección y tratamiento de datos de salud, el artículo 4 de la Ley 26.529 solo permite la transmisión de esta información a terceros con la autorización del paciente. La excepción a esta regla está en el párrafo único del citado artículo, que prevé la posibilidad de transmitir la información a terceros –representante legal, cónyuge, conviviente, cuidador o familiares hasta el cuarto grado de consanguinidad– solo en caso de la incapacidad del paciente o imposibilidad de comprender la información.

Vale la pena decir que los profesionales de la salud están eximidos de la autorización –consentimiento– del paciente en casos de grave peligro para la salud pública o en situación de emergencia, con grave peligro para la salud o vida del paciente, y no pudiera dar el consentimiento por sí o a través de sus representantes legales (artículo 9 de la Ley 26.529).

La ley en cuestión aún protege la historia clínica del paciente, que, por supuesto, consiste en una gran cantidad de información convertida en datos personales sensibles. Según el artículo 14 de esta Ley:

> El paciente es el titular de la historia clínica. A su simple requerimiento debe suministrársele copia de la misma, autenticada por autoridad competente de la institución asistencial. La entrega se realizará dentro de las cuarenta y ocho (48) horas de solicitada, salvo caso de emergencia.

Además del paciente, la ley en foco (artículo 19) considera legitimados para acceder a la historia clínica el representante legal, el cónyuge o conviviente, los herederos forzosos, en su caso, con la autorización del paciente, salvo que éste

se encuentre imposibilitado de darla, y los médicos y otros profesionales del arte de curar, cuando cuenten con expresa autorización del paciente o de su representante legal. Sobre el acceso a la historia clínica por parte de los herederos, posteriormente se realizará una crítica, ya que se considera posible el acceso a los datos de la persona fallecida.

Actualmente, la principal fuente legal de protección de datos personales en Argentina es la Ley 25.326, de Protección de Datos Personales, promulgada en el año 2000, que tiene por finalidad, de acuerdo con su artículo 1°:

> [L]a protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean estos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.

Recuerda que el artículo 43, párrafo tercero de la Constitución Nacional, asegura que toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística.

El Estado argentino considera que la ley en cuestión es insuficiente para la realidad actual de la revolución tecnológica. Por eso, el Ministerio de Justicia y Derechos Humanos tomó la iniciativa de elaborar un proyecto de Ley de Protección de los Datos Personales para reformar la ley vigente. De acuerdo con la Agencia de Acceso a la Información Pública (2018, p. 1) el desafío de esta tarea consistió en elaborar una nueva normativa destinada a proteger los datos personales, la intimidad y privacidad de las personas, sin ser un obstáculo para la innovación y el desarrollo tecnológico y que, además, cumpliera con estándares internacionales.

Destaca Cerda Silva (2012) que el modelo latinoamericano de protección de datos personales está en un estadio de transición. Años atrás, se verificaba a través de disposiciones constitucionales, a las cuales se incorporaba un mayor o menor número de leyes, lo que hacía de ella una regulación fragmentaria y, en ocasiones, inconsistente. Hoy, en las principales economías de la región, esta protección constitucional se traslapa con una norma general que reglamenta el tratamiento de la información personal, sea o no privada. Como resultado de esa superposición de medidas constitucionales y legales, la protección de los datos personales aparece robustecida en América Latina, si bien aún resta fortalecer el efectivo cumplimiento de la ley (p. 170).

No se puede objetar que la tecnología ha evolucionado en los últimos diecisiete años a un ritmo vertiginoso, impactando en gran medida en la protección de los datos personales. Basta señalar que, por ejemplo, *Facebook* surgió en 2004 y *Dropbox* en 2007 para darse cuenta que el escenario en el que se sancionó la Ley 25.326 cambió radicalmente. Esta nueva realidad de la tecnología ha traído enormes desafíos en el campo del ejercicio de los derechos. Los beneficios son innegables, pero también lo son las nuevas potenciales vulneraciones a la intimidad-privacidad (Agencia de Acceso a la Información Pública, 2018, p. 1).

Por otro lado, actualmente se presenta un nuevo contexto regulatorio internacional en esta materia, especialmente a raíz de la adopción del Reglamento General de Protección de Datos (RGPD) que entró en vigencia el 25 de mayo del 2018 y que se prevé tendrá impacto en la Argentina y parte de la comunidad internacional (Agencia de Acceso a la Información Pública, 2018, p. 1).

Sobre la temática desarrollada, se precisa, que la actual Ley de Protección de los Datos Personales de Argentina trae en su artículo 14, párrafo 4, la posibilidad de que los sucesores universales accedan a los datos personales de las personas fallecidas:

> [A]rtículo 14 (Derecho de acceso).
> 1. El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes.

> (...)
> 4. El ejercicio del derecho al cual se refiere este artículo en el caso de datos de personas fallecidas le corresponderá a sus sucesores universales.

Explican Ordelin y Boff (2019, p. 46) que, en la Argentina, a partir de lo previsto en el artículo 14.4 de la Ley 25.326 (Ley de Protección de los Datos Personales), los sucesores universales pueden ejercer el derecho de acceso a los datos de las personas fallecidas, aunque la norma no establece el alcance de este acceso ni como se realizará el mismo.

Ordelin y Boff (2019), en este sentido, observan:

> [E]l artículo 34 de la nueva versión del anteproyecto de Ley de Protección de Datos Personales, resultado de la consulta pública de febrero de 2017, contempla la posibilidad de que el ejercicio de los derechos de acceso, de rectificación, oposición, supresión, valoraciones personales automatizadas y portabilidad de datos personales puedan ser ejercidos por los sucesores universales del titular de los datos. (pp. 46-47).

También para Ordelin y Boff (2019, p. 47) según el artículo 20.2 del citado anteproyecto, estas mismas personas están legitimadas para ejercer la acción de habeas data por el titular de los datos afectados. Entre los legitimados para el ejercicio de los derechos se encuentran los causahabientes siempre y cuando acrediten tal condición.

En cuanto a las acciones que se deben utilizar para la protección de los datos personales, el artículo 33 de la ley actual trae sus posibilidades:

> [1]. La acción de protección de los datos personales o de hábeas data procederá:
> a) para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos;
> b) en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización.

En el proyecto de Ley de Protección de los Datos Personales resultado de la consulta pública de febrero de 2017 se establece expresamente en los artículos 34 (párr. 4°) y 81 (párr. 1°), que, en el caso de las personas humanas fallecidas, los derechos y la acción podrán ser ejercidos por sus sucesores universales.

Un punto importante para este trabajo es que la misma ley, en el artículo 17, párrafo 1, otorga a los administradores de datos el derecho a negarse a proporcionar acceso, eliminación o modificación, siempre que la denegación se funde para proteger los derechos o intereses de terceros:

> [A]rtículo 17. (Excepciones).
> 1. Los responsables o usuarios de bancos de datos públicos pueden, mediante decisión fundada, denegar el acceso, rectificación o la supresión en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros.

Esto abre la posibilidad de denegar el acceso, la rectificación o la supresión de los datos personales, siempre que esto ocurra de manera justificada. Tal posibilidad puede dar lugar, según el caso, a la denegación de acceso, rectificación o supresión de los datos de personas fallecidas, incluidos a los sucesores, si esta medida viola los derechos o intereses de terceros.

La medida autorizada en el artículo en cuestión puede ser una alternativa para la protección de datos de personas fallecidas. Como se verá en el próximo capítulo de este trabajo, algunas redes sociales utilizan acciones similares para denegar el acceso a los datos de los usuarios fallecidos. Sin embargo, esta medida no garantiza la seguridad jurídica, ya que transfiere la facultad de decisión sobre los derechos de acceso, rectificación o supresión de datos a agentes privados. Estos agentes pueden tener varios intereses en mantener la confidencialidad de los datos personales y, en consecuencia, no ser imparciales en la toma de decisiones.

La actual Ley Argentina de Protección de los Datos Personales, ciertamente antigua, espera una reforma para su adaptación al derecho internacional, y a la realidad presente de la revolución tecnológica. Sin embargo, el país no le ha dado

el impulso necesario al tema. Faliero (2018, p. 70) señala al respecto, que se espera que el futuro régimen de protección de datos en la Argentina ofrezca un entorno tuitivo robusto y sólido, que enaltezca la garantía y el ejercicio de los derechos humanos fundamentales en juego.

Debido al retraso en la actualización de la Ley de Protección de los Datos Personales y la intensificación de la dependencia digital provocada por la Pandemia COVID-19, han surgido nuevos proyectos de ley en un intento por actualizar la legislación en la materia. A modo de ejemplo, en una consulta realizada en el sitio *web* de la Cámara de Diputados de Argentina, utilizando como parámetros el término “datos personales” y el período del 01/01/2020 al 24/12/2020 –fecha de la consulta–, se observan 22 proyectos.

La mayoría de estos proyectos de ley se ocupan de disposiciones sobre la modificación de artículos de la Ley de Protección de los Datos Personales vigente o sobre la edición o actualización de leyes independientes que, de alguna manera, se ocupan de la protección de datos personales. Pero el principal es el Proyecto de Ley 6234-D-2020, que prevé la derogación de las leyes 25.326, 26.343 y 26.591. Este proyecto de ley, presentado a la Cámara de Diputados de Argentina el 17 de noviembre de 2020, hasta la conclusión de este el trabajo se encontraba en las etapas iniciales de procesamiento. Por esta razón, no fue objeto de este estudio.

3 La legislación brasileña sobre la protección de los datos personales

En Brasil, después de la publicación de la Ley 13.709 del 14 de agosto de 2018, que establece la protección de datos personales, aún es evidente que la regulación del tema por parte del sistema legal local es insuficiente. Esta ley, a lo largo de sus 65 artículos, no puede disciplinar el tema exhaustivamente, dejando una serie de situaciones, sin la protección legal adecuada. Por ello, la misión del poder judicial es tratar de remediar estas lagunas que no se han llenado. No obstante, y antes de entrar en este punto, es importante que se conozcan las

normas brasileñas de protección de datos, previas a la Ley 13.709 (Rodovalho, 2021, pp. 27-28).

Hemos sostenido (Rodovalho, 2021, p. 28) que, en primer plano, la protección de datos brasileña encuentra en la Constitución Federal de 1988 su fundamento jurídico más importante. Aunque no trata específicamente el tema, la disposición contenida en el artículo 5, X, que garantiza la inviolabilidad de la intimidad, privacidad, honor e imagen de las personas, garantizando el derecho a una indemnización por daños materiales o morales derivados de su violación, se utiliza de manera amplia y pacífica como base para la toma de decisiones sobre protección de datos personales.

Enseña Mendes (2014, p. 141) que, en el marco no constitucional, la primera ley que trató la intimidad-privacidad y la protección de los datos personales de una manera moderna y con vistas a tratar las nuevas tecnologías de procesamiento de datos fue sin duda el Código de Defensa del Consumidor (Ley 8.078, de 11/09/1990).

Mendes continúa (2014) explicando:

> [A] partir de la lectura del artículo 43 de este documento legal se desprende que el Código autoriza el funcionamiento de las bases de datos y registros de consumidores, siempre que se cumplan ciertos preceptos para la protección de la privacidad del consumidor, a saber: (a) la posibilidad de acceder a toda la información existente sobre el consumidor (derecho de acceso); (b) los datos archivados deben ser objetivos, claros, veraces y en un lenguaje fácil de entender (principio de calidad de datos); (c) la necesidad de comunicar la apertura del registro o el registro de datos personales del consumidor (principio de transparencia); (d) obligación de la base de datos de corregir los datos de inmediato (derecho de rectificación y cancelación); y (e) límite de tiempo para el almacenamiento de datos personales (principio de olvido). (pp. 142-143).

En cuanto a la disposición legal en foco, Benjamin *et al* (2005, p. 40) agregan que se inspiró en los estándares estadounidenses del *National Consumer Act* y del

Fair Credit Reporting Act en línea con importantes principios internacionales de protección de datos personales.

Señalamos (Rodovalho, 2021, p. 29) que una norma que generalmente se ocupa de la protección de datos en Brasil es el Código Civil de 2002, que, aunque surgió en un momento de rápida expansión tecnológica, no logró regular el tema de manera más amplia**,** limitándose en sus artículos 20 y 21**,** a la protección del uso de la imagen, la intimidad y privacidad, sin mencionar los medios tecnológicos.

El citado artículo 20 dice lo siguiente:

> [S]alvo autorización, o de ser necesario para la administración de justicia o el mantenimiento del orden público, se podrá prohibir la divulgación de escritos, la transmisión de la palabra, o la publicación, exhibición o uso de la imagen de una persona, a solicitud de ésta y sin perjuicio de la indemnización que corresponda, si alcanzan honor, buena fama o respetabilidad, o si se destinan a fines comerciales.
> Párrafo único. Cuando se trate de fallecidos o ausentes, el cónyuge, los ascendientes o los descendientes están legitimados para solicitar esta protección.

El artículo 21 dispone que la vida privada de la persona natural es inviolable, y el juez, a solicitud del interesado, adoptará las medidas necesarias para prevenir o dar por terminado un acto contrario a esta regla.

A pesar del innovador capítulo sobre el derecho a la personalidad, el código dedicó solo un artículo a la privacidad, que ha merecido críticas por ser demasiado vago y genérico, y solo reproducir lo que el texto constitucional ya proporciona (Schreiber, 2011, p. 136)

En la evolución legislativa brasileña sobre protección de datos, se publica la Ley 12.414 (09/06/2011), que regula la formación y consulta de bases de datos con información de pago, de personas físicas o jurídicas, para la formación de registros de crédito. Este diploma legal estableció el registro positivo que, según Góis (2017, párr. 83), no logró su efectividad social, dada la falta de adhesión de las personas para registrarse en la base de datos. Inicialmente, el artículo 12 de la ley en cuestión disponía que, cuando lo solicite el cliente, las instituciones

autorizadas para operar por el Banco Central de Brasil proporcionarán las bases de datos indicadas con información sobre sus operaciones crediticias.

Esta facultad de integración en el registro positivo, no generó interés en las personas, lo que obligó a un cambio legislativo que nuevamente planteó preocupaciones sobre la protección de datos. De conformidad con la Ley Complementaria 166 (08/04/2019), el artículo 12 de la Ley de Registro Positivo se modificó para hacer obligatoria la integración del consumidor brasileño en el Registro Positivo (Rodovalho, 2021, pp. 29-30).

Mendes (2014) advierte:

> [D]e acuerdo con el Código de Protección al Consumidor, la Ley no. 12.414/2011 establece el principio de la calidad de los datos personales, así como los derechos de acceso a datos, rectificación y cancelación. Además, delimita el propósito para el que se pueden recopilar y utilizar los datos, al afirmar que la información almacenada en las bases de datos solo se puede utilizar para la 'realización de análisis de riesgo de crédito del consumidor' o para 'subsidiar la concesión o extensión de crédito y la venta de cuotas u otras transacciones comerciales que implica riesgo financiero para el consultor'. En este sentido, está claro que estos datos están prohibidos para marketing directo o cualquier otra actividad no mencionada en la ley. (pp. 145-146).

Aunque el Registro Positivo se ha convertido en obligatorio, aún es notable, según Mendes (2014, p. 146), que esta ley consolida la evolución de un concepto de autodeterminación informativa en el sistema legal de Brasil, al establecer mecanismos individuales de control sobre sus datos, asignándole el poder de decidir si le interesa o no integrar esta base de datos, y cuándo desea cancelarlo.

Otro marco legislativo importante en la evolución de la protección de datos en Brasil fue la aparición de la Ley 12.527, el 18 de noviembre de 2011, que regula el acceso a la información pública en el país. Según Mendes (2014, p.148), la ley de acceso a la información es parte del contexto internacional de proporcionar más transparencia a la administración pública, ampliar el control de los ciudadanos sobre el Estado y hacer realidad el derecho fundamental a la información garantizada por la Constitución.

Bottrel (2018, p. 2) sugiere que el interés en ejercer el derecho de acceso a la información de las entidades públicas está justificado, ya que creemos que la implementación de una ley y el reconocimiento de un derecho dependen no solo de su aprobación, sino también de su uso por la sociedad.

Esta ley cubre todos los poderes - Legislativo, Ejecutivo y Judicial - y niveles de gobierno - federal, estatal y municipal, incluido el Distrito Federal. La Ley de Acceso a la Información establece que la regla es el acceso, y la confidencialidad es la excepción, un ejemplo de esto es el caso de la información personal o información relacionada con la seguridad nacional (Bottrel, 2018, p. 4).

El objetivo es alcanzar un estado abierto, en el que haya una sincronización del conocimiento de quien posee el poder y quien otorga el poder (Silveira, 2012, p. 31). El acceso a la información pone al ciudadano en un pie de igualdad con la administración pública y es parte de la fuerza democratizadora de la transparencia y la publicidad (Rodrigues, 2014, p. 94). Para Bottrel(2018, p. 5), la legislación brasileña está bien evaluada, y tiene como principales fortalezas el alcance de las esferas, incluidos los tres poderes y niveles de gobierno, y la certeza de que el secreto es la excepción.

Sobre la protección de datos personales, Mendes (2014) explica:

> [P]or un lado, el derecho de acceso a la información pública fortalece el concepto de protección de datos personales al reforzar la comprensión de que los ciudadanos tienen derecho a acceder a sus datos personales en poder de la Administración Pública (acceso del individuo a sus datos personales). Por otro lado, el derecho a la protección de datos personales puede verse como una limitación del derecho de acceso a la información, ya que, por regla general, los terceros no pueden tener acceso a los datos personales del titular sin su consentimiento; solo bajo condiciones específicas es posible. (pp. 148-149).

Citando las disposiciones presentadas en el artículo 31, Mendes (2014) enseña:

> [L]a ley de acceso cumple un papel importante en la búsqueda de trazar los límites entre el derecho a la privacidad y el derecho a la información, estableciendo

> ciertos criterios según los cuales el acceso a los datos puede darse sin el consentimiento del titular. (p. 153).

Machado Gonçalves y Varella (2018, p. 532) enfatizan que la disponibilidad de datos confidenciales por parte de la administración pública es un tema que debe desarrollarse legalmente y mediante regulaciones específicas, porque está asociado con la confianza y la credibilidad de las instituciones y el deber de la publicidad del gobierno. Además, la creación de una política nacional de protección de datos personales es indispensable en la actualidad para evitar la violación de los derechos fundamentales.

El sistema jurídico brasileño de protección de datos personales comenzó a integrarse, a partir de 2012, con otra norma de importancia, como la Ley 12.737 (30/11/2012), que modificó el Código Penal para incluir delitos informáticos. Esta ley se denominó “Lei Carolina Dieckmann” en honor a una actriz brasileña que tuvo fotos íntimas expuestas en Internet luego de la violación de un dispositivo informático.

A través de esta Ley, el Código Penal brasileño añadió los artículos 154-A y 154-B y modificó las redacciones de los artículos 266 y 298. La novedad más importante estuvo a cargo del delito incluido en el artículo 154-A, mientras que las otras enmiendas se ocuparon de proceso penal y actualización de delitos que ya existían.

El texto de este artículo comenzó a considerar como delito la invasión de un dispositivo informático, mediante una violación indebida del mecanismo de seguridad y con el propósito de obtener, manipular o destruir datos o información sin la autorización expresa o tácita del propietario del dispositivo o instalar vulnerabilidades para obtener una ventaja ilegal. La pena prevista es de prisión, de 3 meses a 1 año, y multa.

Andréa, Arquite y Camargo (2020) critican esta ley, diciendo que el intento de establecer la criminalización de la invasión de dispositivos sin autorización se convierte en un fracaso, pues también existe la hipótesis de que el propio lesionado entrega, por sí solo, su máquina. Queda […] la ausencia de protección jurídica en cuanto al uso de datos personales por un tercero sin autorización, o

autorización genérica, sin finalidad específica. Por ejemplo, la autorización para acceder a un documento en la nube tras la entrega del login y la contraseña por parte del perjudicado impide la aplicación de la legislación si se accede a algún documento indebido de forma culpable (p.8).

Explicamos (Rodovalho, 2021, p. 32) que, en un intento más incisivo de regular las políticas de flujo de datos, el Estado brasileño aprobó la Ley 12.965 (23/04/2014), que establece principios, garantías, derechos y deberes para el uso de Internet en Brasil. Esta ley fue nombrada Marco Civil de Internet.

Tomasevicius Filho (2016, p. 276) señala que aunque el Marco Civil de Internet fue ampliamente celebrado por ser la primera ley en el mundo para regular los derechos y deberes de los usuarios de la red, no habrá cambios sustanciales, ya que no ha agregado prácticamente nada a la legislación vigente.

El autor citado (p. 276) continúa criticando la expectativa creada por la discusión de esta ley, que se debió a la creencia errónea de que las normas contenidas en la Constitución Federal, el Código Civil, el Código Penal, los Códigos de Procedimiento Civil y Penal, el Código de La Protección del Consumidor, el Estatuto del Niño y el Adolescente y la Ley de Interceptación de Comunicaciones (Ley 9.296/96) no tendrían aplicación en las relaciones legales establecidas en Internet.

En contraste con estas afirmaciones, Correa de Barros y Flain (2016, p. 10) encuentran que el Marco Civil de Internet, al establecer en el Capítulo II, los derechos y garantías de los usuarios, ha dado un paso importante en la regulación de las relaciones en el espacio virtual. Proteger la privacidad de las comunicaciones y proteger los datos personales son innovaciones importantes que garantizan la seguridad del usuario. Es de destacar, la amplia protección de la libertad de expresión, uno de los valores sociales más relevantes.

En la misma línea, Rodrigues Rezende y Rodrigues de Lima (2016, p. 150), afirman que el Marco Civil de Internet fue un proceso pionero en el país, al que asistieron ciudadanos y entidades representativas, lo que contribuyó a la creación de una ley, y lo más importante, una ley que los beneficia directamente. Estos autores continúan aclarando que, quizás por esta razón, el contenido abordado,

incluso si se considera sofisticado sobre las pautas que componen el texto, presenta para algunos académicos un carácter generalista y superficial en comparación con otros países. Igualmente, se puede considerar que Brasil tiene hoy una de las leyes más progresistas del mundo sobre el uso de Internet.

Destacan Correa de Barros y Flain (2016, p. 10) que el segundo capítulo del Marco Civil de Internet trata, en los artículos 7º y 8º, de los derechos y garantías de los usuarios.

Se supone que el acceso a Internet es esencial para el ejercicio de la ciudadanía; por lo tanto, el usuario tiene derecho a que se proteja su privacidad e intimidad, y, en caso de violación, el derecho a compensación; inviolabilidad y confidencialidad del flujo de comunicaciones a través de Internet y comunicaciones privadas almacenadas, excepto por orden judicial (Rodrigues Rezende y Rodrigues de Lima, 2016, p. 147).

Sobre el mantenimiento de la privacidad de los datos personales y las comunicaciones privadas, existe preocupación acerca de la identificación individual del usuario en los casos en que se le considera responsable de delitos en Internet. El Marco Civil no especifica como los proveedores de Internet y de aplicaciones deben almacenar los datos de los usuarios ya que, si los datos técnicos necesarios no se mantienen adecuadamente, será difícil identificar delincuentes en Internet (Rodrigues Rezende y Rodrigues de Lima, 2016, pp. 149-150).

Al mismo tiempo que el Marco Civil estipula las normas sobre protección de datos, se ve claramente la precaución de no ingresar competencias que se ajusten a una futura ley de datos personales esenciales (Menezes Souza, 2018, p. 19).

Hemos señalado (Rodovalho, 2021, p. 34) que, en vista del controvertido Marco Civil de Internet y la intensificación de la revolución tecnológica, fue necesaria la Ley 13.709 (14/08/2018), que se ocupa de la protección de datos personales y modifica el Marco Civil de Internet. Esta ley es el último intento de regular la protección de datos en Brasil, ya que crea la política nacional sobre protección de datos personales.

Santiago (2018, párr. 5) explica que, en Brasil, la entrada en vigor de la Ley General de Protección de Datos tiene el objetivo de crear un marco regulatorio moderno, inspirado en gran medida por el Reglamento Europeo; señalándose entre otros, el de colocar a la Nación brasileña, en la lista de países y organizaciones internacionales que brindan una protección adecuada a los datos personales.

Por lo tanto, se crearon una serie de obligaciones para las empresas relacionadas a la recopilación, el uso y las garantías de integridad de los datos personales que deben observarse, bajo pena de fuertes sanciones. Asimismo, la ley mencionada confiere derechos a los titulares de datos personales que pueden ejercerse contra cualquier empresa o entidad pública que posea dicha información. En este sentido, si los datos personales se han convertido indudablemente en un activo valioso, pueden dar lugar, si se administran incorrectamente, a una responsabilidad importante para quienes los poseen (Santiago, 2018, párr. 6).

La Ley General de Protección de Datos establece una serie de derechos que garantizan: el respeto a la privacidad; autodeterminación informativa; libertad de expresión, información, comunicación y opinión; la inviolabilidad de la intimidad, el honor y la imagen; desarrollo e innovación económica y tecnológica; libre empresa, libre competencia y protección del consumidor; y los derechos humanos, el libre desarrollo de la personalidad, la dignidad y el ejercicio de la ciudadanía por parte de las personas físicas. En este contexto, la ley en foco disciplina de manera muy amplia, en el Capítulo 3, los derechos del interesado (Rodovalho, 2021, p. 35).

Santiago (2018, párr. 11) enumera los principales derechos del titular: acceso y corrección de datos incompletos, inexactos u obsoletos; anonimizar sus datos, bloquear o eliminar datos innecesarios, excesivos o tratados en violación de las disposiciones de la ley; portabilidad de datos a otro proveedor de servicios o productos (por ejemplo, bancos, para facilitar la apertura de cuentas corrientes, aseguradoras, etc); la eliminación de datos personales procesados con el

consentimiento del titular; la información de entidades públicas y privadas con las que se compartió el uso de datos; y la revocación del consentimiento.

El autor citado (2018, párr. 10) explica que el consentimiento se convierte en la mejor manera de legitimar el procesamiento de datos personales. Debe ser explícito y, cuando se solicite en medio de un contrato que contenga otros elementos, debe estar contenido en una cláusula separada. El consentimiento puede ser revocado en cualquier momento por el interesado. Otras razones también legitiman el procesamiento de datos personales (por ejemplo: cumplimiento de obligaciones legales o reglamentarias, cumplimiento del contrato del que es parte el titular, y estudios del organismo de investigación, entre otros).

Según lo que hemos defendido (Rodovalho, 2021, p. 36), es en este estándar que Brasil busca actualmente encontrar una regulación más efectiva de la protección de datos. Su redacción, incluso antes de que entrara en vigor en su totalidad, ya estaba incompleta. Tanto es así que el texto legal ya ha sufrido varios cambios después de su publicación.

Dentro de las relaciones laborales, según Reani (2018, párr. 30), los sistemas que permiten a los empleadores controlar quién puede ingresar a sus instalaciones y/o ciertas áreas también pueden rastrear las actividades de los empleados. Aunque estos sistemas existen desde hace varios años, se han introducido nuevas tecnologías para controlar y monitorear la actividad laboral.

Sin embargo, el monitoreo continuo de la frecuencia de los empleados y los tiempos exactos de entrada y salida no pueden justificarse, si estos datos también se usan para otro propósito (Reani, 2018, párr. 32).

Concluimos diciendo (Rodovalho, 2021, p. 120) que la evolución legislativa brasileña en materia de protección de datos muestra que la regulación del tema nunca ha sido fácil, y, dada la intensa velocidad con la que la revolución tecnológica crea nuevos hechos legales, parece que la ley no puede delimitar las reglas.

América Latina está adoptando leyes que reglamentan el tratamiento de datos personales de un modo integral, esto es, en las que sea comprendido el procesamiento de información tanto por el sector público como por el privado.

Diversas razones explican este fenómeno: los nuevos bríos democráticos, que invitan a brindar adecuada protección a los derechos de las personas; el afán de minimizar la incertidumbre de un modelo de protección basado solo en disposiciones constitucionales; pero más significativamente, la aspiración de transformarse en un país que brinda un nivel de protección adecuado, de acuerdo con los estándares promovidos por la Unión Europea, a efectos de acceder a la transferencia de datos personales desde esta y, con ello, facilitar la inversión en aquellos nichos de mercado que suponen tratamiento de datos provenientes de aquella (Cerda Silva, 2012, p. 170).

La complejidad de la protección de datos va más allá de las fronteras de todos los países, convirtiéndose en un problema universal que la comunidad internacional debe abordar colectivamente. Es en el panorama legislativo aquí presentado donde se desarrolla el problema central de esta tesis. A partir de las normas existentes, la evolución legislativa y la dificultad de la ley para seguir la tecnología, se intentará proponer una posible solución para la protección de los datos de las personas fallecidas.

4 El tratamiento en la protección de los datos personales por los tribunales argentinos y brasileños

Incluso antes de la revolución tecnológica experimentada hoy en día, la protección de la intimidad y privacidad fue objeto de un debate en profundidad en los tribunales, que siempre pone en conflicto el derecho a la información y la publicidad, con los derechos de la personalidad. En Brasil y Argentina, los casos más emblemáticos involucraron a figuras públicas, que tenían exposiciones no autorizadas de sus imágenes y vidas privadas.

Uno de los casos más conocidos en Argentina fue el de la modelo María Belén Rodríguez, que, en 2005, tuvo un uso no autorizado de su imagen en Internet, vinculada a contenidos eróticos y pornográficos. La modelo buscó la responsabilidad de los motores de búsqueda de Internet al ejemplo de *Google* y *Yahoo*, lo que facilitó la transmisión en línea de material no autorizado.

En este caso la Corte Suprema de la Nación Argentina ha dicho que:

> N]o debe perderse de vista que el servicio de imágenes constituye una herramienta de búsqueda automatizada que muestra —a través de los denominados "*thumbnails*"— una copia reducida de las imágenes que existen en la *web* relacionadas con las palabras ingresadas y con expresa referencia al sitio en el que ellas se encuentran alojadas. De modo que la conducta que llevan a cabo los buscadores no es susceptible de ser encuadrada en la norma citada – art. 31 de la ley 11.723–, pues consiste en una simple recopilación automática de vistas en miniatura que solo tiene por finalidad permitir a los usuarios acceder a las páginas de Internet que contienen las imágenes originales. (CSNA. R. 522. XLIX. REX Rodríguez, María Belén c/ *Google* Inc y otro Y OTROS s/daños y perjuicios, considerando 21).

La Corte Argentina entendió que no existía responsabilidad de los demandados, por ser meros intermediarios cuya única función es servir de enlace con las publicaciones ya disponibles en Internet. Pero, advierte Molina Quiroga (2018) que la existencia o no de responsabilidad por los contenidos publicados en la red, y en su caso, el factor de atribución aplicable, así como el momento a partir del cual nace la eventual responsabilidad divide a la doctrina y jurisprudencia nacionales, aunque el pronunciamiento de la Corte Suprema en el caso "Rodríguez Belén v. Google", reiterado en caso "Gimbutas c. Google s/daños y perjuicios" parece haber inclinado el fiel de la balanza hacia el factor subjetivo. (p.176).

En Brasil, un caso que tuvo repercusión nacional, que también involucró derechos personalísimos y buscadores de Internet, fue el caso de la presentadora de televisión Maria da Graça Xuxa Meneghel (Xuxa). En la acción propuesta en 2010, la presentadora buscó el "Derecho al Olvido" de las imágenes de una película emitida en 1982, donde protagonizó una escena erótica con un menor de 12 años de edad. Para hacerlo, demandó al motor de búsqueda *Google*, con el fin de eliminar los resultados de búsquedas realizadas con su nombre vinculado al término "pedofilia".

En otro caso, el Supremo Tribunal Federal brasileño sostuvo que la empresa anfitriona de sitios en la red mundial de ordenadores debe fiscalizar el contenido publicado en sus dominios electrónicos y retirar del aire las informaciones reputadas ofensivas, sin necesidad de intervención del Poder Judicial (STF. ARE 660861, juzgado el 22/03/2012, pp. 2-3).

Sin embargo, en el caso de la presentadora brasileña, la Corte Suprema no enfrentó directamente el mérito, considerando que no se utilizaron los medios procesales de impugnación apropiados (STF. Segunda Turma. Ag. Reg. na Reclamação 15.955, juzgado en 15/09/2015). Por lo tanto, confirmó la decisión de la instancia anterior, del Superior de Tribunal de Justicia, que había decidido lo siguiente:

> Los proveedores de búsqueda realizan sus búsquedas dentro de un universo virtual, cuyo acceso es público y sin restricciones, es decir, su función está restringida a la identificación de páginas *web* donde ciertos datos o información, incluso si son ilícitos, se transmiten libremente. Por lo tanto, a pesar de sus motores de búsqueda facilitan el acceso y la consiguiente difusión de páginas de contenido potencialmente ilegal, el hecho es que estas páginas son públicas y conforman la Internet y, por lo tanto, aparecen en el resultado de los sitios de búsqueda (STJ. Tercera Turma. Resp. 1.316.921, juzgado en 26/06/2012, considerando 5).

En otra parte de la misma decisión, la Corte Superior de Justicia de Brasil también declaró:

> No se puede, con el pretexto de impedir la propagación de contenido ilegal u ofensivo en la *Web*, suprimir el derecho de la comunidad a la información. Después de considerar los derechos involucrados y el riesgo potencial de violación de cada uno de ellos, el equilibrio debe depender de garantizar la libertad de información garantizada por el artículo 220, § 1, de CF/88, especialmente teniendo en cuenta que *Internet* es hoy un vehículo importante para los medios de comunicación (Considerando 7).

Finalmente, la decisión confirmó que, en este caso, no hubo responsabilidad de los buscadores de Internet por los daños causados por las páginas *web* que aparecen en los resultados de búsqueda:

> Una vez que se hayan cumplido los requisitos para la exclusión de una determinada página virtual de la *web*, bajo el alegato de ofrecer contenido ilícito u ofensivo –en particular la identificación de la URL de esa página– la víctima no tendrá interés en actuar contra el proveedor de búsqueda, por absoluta falta de utilidad jurisdiccional. Si la víctima ha identificado, vía URL, al autor del acto ilícito, no tiene por qué demandar a quien solo facilita el acceso a este acto, el cual, hasta entonces, ha estado disponible públicamente en la red para su divulgación. (Considerando 8).

Tanto en el caso de la modelo argentina, como en el caso de la presentadora brasileña, es evidente el conflicto que existe entre el derecho a la información y derechos de personalidad. En ambos casos, los Tribunales decidieron de manera similar, eximiendo los buscadores de Internet de responsabilidad por las publicaciones disponibles en la *web* y que causen perjuicios a derechos como la imagen, el honor, la intimidad y la privacidad.

Lejos del mundo de los famosos, un reciente fallo de un tribunal argentino ilustra la crisis de los derechos a la intimidad y privacidad potenciados por los medios tecnológicos. El caso involucra el acceso no autorizado a los datos de un teléfono móvil por parte de una persona (Sra. S.) perteneciente al mismo grupo familiar que el propietario del dispositivo (G.). En ese acceso, la Sra. S. descubrió la supuesta comisión de delitos vinculados a menores representando actividades sexuales explícitas, entregando el dispositivo a la autoridad policial. Este hecho inició un proceso penal. La defensa de G. solicitó la exclusión de las pruebas obtenidas mediante el acceso ilícito a los datos de su celular, por violación a la intimidad y la privacidad.

En la sentencia del caso, la Sala I de la Cámara Nacional en lo Criminal y Correccional entendió que no hubo violación de la intimidad y privacidad bajo el siguiente argumento:

> [A] su vez, cabe señalar que la Sra. S. encontró el celular en el domicilio en el que aún convivía con G., de

> este modo consideramos que también asiste razón al Sr. juez de primera instancia en cuanto a que la intimidad del imputado se encontraba en cierta medida limitada, dado que esa situación desdibuja los límites y restringe en cierta medida las expectativas de privacidad (CNCrim. y Correc., sala I, 19/05/2020. - G., E. D. s/ Nulidad, p. 8).

Al comentar el caso en cuestión, Schiavo (2020, p. 8) defiende que la Cámara formula dos argumentos que no son necesariamente compatibles. En el primero de ellos precisa que la intromisión en la información no tenía el propósito de transgredir los espacios de privacidad, mientras que en el segundo se sostiene que la señora S. convivía con G., de tal modo que la relación de intimidad "desdibuja los límites y restringe en cierta medida las expectativas de privacidad".

Concluye Schiavo (2020, p. 8), señalando, que el segundo argumento que se proporciona impresiona inadecuado y en determinados contextos podría resultar sumamente peligroso, pues, aunque pudiera ser evidente que la convivencia en un domicilio torna más estrechas las expectativas de privacidad, aun allí existen espacios donde se conserva pleno dominio de sus límites, como puede ser un diario íntimo, las comunicaciones por mensajería electrónica presente en el aparato telefónico, su agenda de contactos y la galería de imágenes.

El hecho es que, aunque distantes en el tiempo y el espacio, estos casos sirvieron para ilustrar la crisis de los derechos personalísimos de imagen, intimidad y privacidad con la llegada de Internet. El mayor problema es que con la virtualización de la vida, la crisis de intimidad-privacidad ha afectado a todas las personas, no siendo una preocupación exclusiva de los usuarios más expuestos.

Según Becerra y Zárate (2015):

> [E]l interés jurídico protegido que trata sobre la reserva de la vida privada, la honra y la reputación, ha mutado con los cambios provocados por Internet y la sobreexposición de la vida privada, es innegable la necesidad de repensar el derecho, los casos jurisprudenciales más destacados hacen alusión a la vida de los artistas y famosos, sin embargo, hoy la vida de cualquier persona sin distinción de sexo y edad, puede sufrir un ataque en su dignidad. (p. 218).

Es en este contexto que la protección de datos personales adquiere una importancia enorme, lo que justifica la carrera mundial antes mencionada para la protección de datos que viajan a través de Internet. Argentina y Brasil no están fuera de esta carrera, ya que están ajustando su legislación para proporcionar mayor seguridad y responsabilidad a los datos personales.

En el caso de Argentina, el país está esperando el final del proceso legislativo en el Congreso Nacional de su nueva Ley de Protección de los Datos Personales. En Brasil, ya existe una nueva Ley de Protección de Datos Personales sancionada por el Poder Ejecutivo, que es la Ley 13.709, de 14 de agosto de 2018.

Debido a la adaptación legislativa actual, es natural que los poderes judiciales de Argentina y Brasil aún no tiene una posición consolidada sobre la violación de los datos personales desde la perspectiva de la nueva legislación.

Villegas Carrasquilla (2012, p. 144) aclara que no se encuentran en la legislación argentina normas especiales sobre el derecho a la intimidad y privacidad en relación con Internet. En ese sentido, los tribunales de justicia argentinos han considerado equiparable el tratamiento que se le debe dar a estos derechos en Internet al tratamiento que se le otorga en otros medios, tales como la prensa o la televisión.

En efecto, según Addati (2020, p. 70), la carencia de una ley que regule el “entorno en línea” y de una doctrina judicial uniforme permite que cada juez natural evalúe la cuestión desde su punto de vista, algunas veces aplicando con mayor vigor la protección a la garantía de la libertad de expresión mientras que en otros otorgando preeminencia a la protección a los derechos personalísimos.

Igualmente, más allá de lo señalado por los autores citados, preciso respecto de Internet, que en el orden regulatorio, la República Argentina comenzó con las Resoluciones de la Secretaría de Comunicaciones 2814/1997 y 499/1998, las que incluyeron el servicio de acceso a Internet, dentro de los servicios de telecomunicaciones. Luego, el Decreto 554/1997 declaró de Interés Nacional el acceso de los habitantes de la República Argentina a la red mundial Internet en condiciones sociales y geográficas equitativas, con tarifas razonables y con

parámetros de calidad acordes a las modernas aplicaciones de la multimedia (artículo 1º). Posteriormente, el Decreto 1279/1997 dispuso, que el servicio de Internet se considera comprendido dentro de la garantía constitucional que ampara la libertad de expresión, correspondiéndole en tal sentido las mismas consideraciones que a los demás medios de comunicación social (artículo 1°). Al año siguiente, y dentro de las normas que sitúan a Internet fuera del contralor público, la Resolución 1235/1998 de la Secretaría de Comunicaciones exigió, que las facturas emitidas por los Internet Service Provider debían incluir la siguiente inscripción, “El Estado Nacional no controla ni regula la información disponible en Internet. Se recomienda a los padres ejercer un razonable control por los contenidos que consumen sus hijos. Es aconsejable la consulta a su proveedor de servicios de acceso a fin de obtener el correspondiente asesoramiento sobre programas de bloqueo de sitios que consideren inconvenientes”.

En el 2005, la Ley de Servicios de Internet, 26.032, dispuso que “La búsqueda, recepción y difusión de información e ideas de toda índole, a través del servicio de Internet, se considera comprendido dentro de la garantía constitucional que ampara la libertad de expresión”.

El marco normativo sobre la regulación de Internet en la República Argentina, en la actualidad, tiene otros aspectos de relevancia a considerar, a partir de la pandemia por coronavirus, al declararse, por caso, a las *telecomunicaciones*, *Internet fija* y *móvil* y los *servicios digitales*, como servicios *esenciales*, estando en un período del 2020, las empresas prestadoras de los servicios de energía eléctrica, gas por redes y agua corriente, *telefonía fija* y *móvil*, *Internet* y *TV por cable, por vínculo radioeléctrico* y *satelital* impedidas de suspender o cortar los servicios a usuarios/as especificados/as en el Decreto 311/2020, en caso de mora o falta de pago, por considerarlos *centrales* para el desarrollo de la vida diaria, y *medios instrumentales* para la satisfacción de *derechos fundamentales* de la población.

Al poco tiempo, y en las mismas circunstancias producidas por la pandemia, el Decreto 690/2020, ratificado en su validez por el Honorable Senado de la

Nación (Resolución 95/2020), categorizó a los servicios de TIC, como servicios *públicos, esenciales y estratégicos en competencia*.

Respecto de lo señalado sobre la protección de los datos personales, Cerda Silva (2012) aclara que la normativa constitucional no ha sido suficiente para garantizarlos en un adecuado nivel en América Latina. Esto sucede porque dicho resguardo se verifica preferentemente en sede judicial y ello trae aparejado una serie de limitaciones, tales como sus altos costos transaccionales; su ineficacia para prevenir infracciones y su falta de experiencia en temas que, en ocasiones, resultan altamente técnicos. Además, como en los demás países depositarios de la tradición del Derecho Civil, en los países latinoamericanos, los precedentes judiciales carecen de fuerza obligatoria en casos futuros, salvo limitadísimas excepciones (p. 169).

Para Fernández (2019) frente a los avances tecnológicos, la respuesta jurisprudencial ha sido la de intentar preservar el mismo grado de protección de la privacidad que el existente al momento de la adopción del texto constitucional, pero adaptado a los tiempos actuales. Esta discusión está aún en una etapa inicial y será necesario seguir analizando los avances tecnológicos y las soluciones legales tradicionales (p. 69).

En esta línea, algunas decisiones emblemáticas dictadas por los tribunales superiores de Argentina y Brasil sirven de pautas para la defensa de los derechos de la personalidad en tiempos de revolución tecnológica y creciente uso de Internet. En Argentina son ejemplos los conocidos casos: Halabi, Ernesto c/ P.E.N. (CSJN; 24/02/2009); F., D. S. c/ Google Inc. y otro s/ medidas cautelares–incidente (Cámara Nacional de Apelaciones en lo Civil y Comercial Federal, Sala III; 22/04/2016); Franco, Julio César c/ Diario “La Mañana” y/u otros s/ daños y perjuicios (CSJN; 30/10/2007: Fallos: 330:4615); Ponzetti de Balbín, Indalia c/ Editorial Atlántida S.A. s/ daños y perjuicios. (CSJN; 11/12/1984, Fallos: 306:1892); Recurso de hecho deducido por la demandada en la causa Irigoyen, Juan Carlos Hipólito c/ Fundación Wallenberg y otro s/ daños y perjuicios (CSJN; 05/08/2014).

Del mismo modo, en Brasil, son ejemplos de casos de gran repercusión en la materia: Recurso extraordinário 601314/SP, Marcio Holcman c/ União Federal (STF; 24/02/2016); Habeas corpus 168052/SP, Arai de Mendonca Brazao c/ Superior Tribunal de Justiça (STF; 20/10/2020); Recurso ordinário em mandado de segurança 60.531/RO, WhatsApp Inc. c/ Ministério Público do Estado de Rondônia (STJ; 09/12/2020); Recurso especial 1784156/SP, TIM Celular S.A c/ Google Brasil Internet LTDA (STJ, 05/11/2019); y, Recurso especial 1168547/RJ, World Company Dance Show LTDA c/ Patrícia Chélida de Lima Santos (STJ; 11/05/2010).

Sin embargo, ejemplos como los de las decisiones antes mencionadas demuestran que aún no existe una jurisprudencia consolidada sobre la protección de los derechos de la personalidad, en particular la intimidad y la privacidad, en la sociedad de la información. Se justifica aquí que no se profundizará el estudio de los casos citados porque no están directamente relacionados con el tema investigado en este trabajo, que tiene como tema central los derechos a la intimidad y privacidad *post mortem* según la protección de datos personales.

En consulta en el sitio de la Corte Suprema de Brasil, teniendo expresiones parametrizadas “Privacidade e Proteção de Dados Pessoais” y el período de 14 de agosto de 2018 (fecha de publicación de la Ley General de Protección de Datos de Brasil) al 8 de diciembre de 2019 (fecha de consulta), no se ha presentado ninguna sentencia del Tribunal Supremo.

En esta misma consulta, solo aparecieron tres decisiones monocráticas, ninguna de las cuales está directamente relacionada con la violación de la privacidad y la protección de datos personales. La ausencia de sentencias de la Corte Suprema de Brasil se repite cuando los parámetros de la consulta son las expresiones “Lei Geral de Proteção de Dados Pessoais” o “Lei 13.709/2018” y el mismo período de la consulta anterior.

En consulta similar a la Corte Suprema de Justicia de la Nación Argentina, donde se usó la expresión “Privacidad y Protección de Datos Personales” y dado el mismo lapso de tiempo como parámetro, no surgió ninguna decisión. Se obtiene el mismo resultado al consultar las bases de datos de la jurisprudencia de la

Cámara Nacional de Apelaciones en lo Civil y de la Cámara Nacional de Apelaciones en lo Civil y Comercial Federal.

Cuando la consulta se realiza en el sitio del Superior Tribunal de Justicia de Brasil, aparecen algunos juzgados. Si se repiten los parámetros de la primera consulta realizada al sitio de la Corte Suprema, a saber, las expresiones “Privacidade e Proteção de Dados Pessoais” y el período de 14 de agosto de 2018 (fecha de publicación de la Ley General de Protección de Datos Personales de Brasil) al 8 de diciembre de 2019 (fecha de consulta), se presentan tres decisiones.

De las tres sentencias del Superior Tribunal de Justicia encontradas, una se ocupa de la protección de datos y la privacidad de los usuarios de redes sociales, y las restantes se ocupan de la protección de datos personales y la privacidad del consumidor.

La primera sentencia encontrada en la consulta de la jurisprudencia del Tribunal Superior se refiere a una apelación especial de *Facebook*. En la apelación, *Facebook* cuestiona la necesidad de una orden judicial para proporcionar datos de sus usuarios. Basando la decisión en el Marco Civil de Internet de Brasil, la Corte Superior de Justicia dictaminó lo siguiente:

> El Marco Civil de Internet establece que una orden judicial es obligatoria para que los proveedores de acceso y aplicación presenten datos personales y confidenciales a las partes interesadas. Es la protección necesaria y esperada de la privacidad e intimidad de los usuarios de aplicaciones de Internet (STJ. Tercera Turma. Resp. 1.782.212, juzgado en 05/11/2019, considerando 3).

Las dos sentencias restantes, que tienen la misma redacción, se refieren al uso de datos personales del consumidor con el fin de otorgar crédito. Las decisiones, que esta vez se basan en la Constitución Federal, establecen que la protección de datos está estrechamente vinculada a la privacidad e intimidad del consumidor, como se puede extraer del siguiente extracto:

> Los derechos a la intimidad y protección de la privacidad, directamente relacionados con el uso de datos personales por las bases de datos de protección

> de crédito, consagran el derecho a la autodeterminación informativa y están constitucionalmente protegidos en el artículo 5, X, de la Carta Magna, que debe aplicarse en las relaciones entre individuos en virtud de su efectividad horizontal y privilegiada por la imposición del principio de máxima efectividad de los derechos fundamentales (STJ. Tercera Turma. EDcl. en lo REsp 1630659/DF y EDcl en lo REsp 1.630.889/DF, juzgado en 27/11/2018, considerando 7).

Lo que llama la atención en las sentencias encontradas en el Superior Tribunal de Justicia de Brasil es que en ninguna de ellas se menciona, ni siquiera indirectamente, la Ley General de Protección de Datos Personales del país, que ya se había publicado en la fecha de todas las sentencias.

Es cierto que, en las fechas de los juicios, aunque ya existía la referida ley aún no había entrado en vigor en su totalidad, lo que puede justificar la falta y cualquier mención a su respecto. La ausencia de cualquier mención de la nueva ley en las sentencias del Superior Tribunal de Justicia se refuerza al repetir los parámetros de la consulta realizada a la jurisprudencia del Supremo Tribunal Federal, utilizando los términos “Lei Geral de Proteção de Dados Pessoais” o “Lei 13.709/2018” y el mismo período que la consulta realizada allí.

El futuro en la protección de los datos personales es prometedor. Nos plantea y enfrenta con desafíos inconmensurables desde lo técnico y lo legal, y es responsabilidad de los profesionales del derecho velar por el avance y la garantía de los derechos humanos fundamentales que se encuentran en juego, así como por su no regresividad (Faleiro, 2018, p. 69). La falta de una jurisprudencia consolidada en la materia hace que estos desafíos sean aún mayores y requerirá de muchos esfuerzos por parte de todos aquellos que trabajan con la protección de datos personales, hasta que exista una adecuada protección jurídica en la materia.

5 Conclusión

La inserción de la tecnología en las relaciones sociales ha estado ocurriendo a una velocidad que la ley no puede alcanzar. De hecho, es común que la ley

parezca normalizar las situaciones después de que sucedan, y por lo tanto no es diferente con la tecnología.

El problema es que la tecnología avanza hacia la humanidad a una velocidad inalcanzable para el Derecho. En este sentido, en el presente capítulo se ha demostrado que la evolución de la protección legal de los datos personales en Argentina y Brasil no ha sido acompañada con la celeridad que se requiere para su tratamiento y actualización.

La legislación argentina sobre la protección de datos personales requiere de su renovación, desde hace años. Sin embargo, parece que el país no ha atendido debidamente la cuestión, ya que, desde el 2016, no prioriza el procesamiento del proyecto de ley que renovará y normativizar el tema en cuestión hasta el punto de dejar perder el estado parlamentario. La expectativa es que, con la intensificación de la actividad legislativa en la materia, principalmente después de la Pandemia COVID-19, el sistema de protección de datos personales de la Argentina pronto se actualizará, generándose una normativa más completa.

Mientras tanto, las normas antiguas y obsoletas, distribuidas en varias leyes siguen regulando la protección de datos personales sin abordar de manera efectiva los nuevos conceptos y problemas provocados por la revolución tecnológica.

En Brasil, la legislación se actualizó en el 2018, con la aprobación de la Ley General de Protección de Datos Personales. La inspiración para esta ley fue el Reglamento General sobre la Protección de los Datos Personales de la Unión Europea, que debe ser bienvenido, ya que el tema de la protección de los datos personales va más allá de los límites territoriales de cualquier país.

Es importante tener una estandarización normativa internacional. Además, también es en el Reglamento General para la Protección de Datos Personales de la Unión Europea donde se inspira el proyecto de ley argentino, que aún espera la conclusión de los procedimientos en el Congreso Nacional.

Cuando el análisis se realiza en los poderes judiciales de Argentina y Brasil, existe un panorama de incertidumbre sobre la tutela jurisprudencial dada a la protección de datos personales en ambos países. El tema, aunque cada vez más

recurrente en la vida de las personas, aún es escaso en los tribunales superiores, que son responsables de consolidar la jurisprudencia.

La investigación en las bases de datos de estos tribunales en Argentina y Brasil muestra que sus respectivos tribunales aún no han abordado adecuadamente el tema hasta el punto de formar una consolidación de la posición jurisprudencial. La ausencia de sentencias recientes en los tribunales de ambos países demuestra que la cuestión de la intimidad y privacidad relacionada con la protección de datos personales todavía está poco judicializada.

Por lo tanto, se concluye, que Argentina y Brasil, si bien están tratando de consolidar en el mundo legal, el campo de protección de los datos personales, ambos países presentan diferentes escenarios normativos.

Brasil, por su parte, avanzó legislativamente al aprobar la Ley General de Protección de Datos Personales, inspirada en el Reglamento General de Protección de Datos de la Unión Europea, y la creación de la Autoridad Nacional de Protección de Datos. Argentina, en cambio, necesita abordar urgentemente el tema regulatorio, observándose que la demora legislativa desactualizó su proyecto de ley –como lo explicara en el presente capítulo–, requiriéndose por ello, de su reformulación.

Capítulo III: Los derechos a la intimidad y privacidad en Argentina y Brasil respecto a los datos e informaciones privadas de las personas vivas guardadas en Internet

1 Introducción

En este capítulo se analizará el comportamiento de la sociedad con el panorama existente de protección de datos personales. A pesar de la existencia de normas que se aplican al tema desde hace algunas décadas, la consolidación de sistemas jurídicos de protección de datos personales solo comenzó a existir después de la llegada de la revolución tecnológica.

Es necesario analizar la importancia real de los datos personales para evaluar también si la inquietud reportada aquí, tiene una causa justificada en su existencia. Por ello, el objeto central de este capítulo es comprender el valor real que tienen los datos personales, en un intento de medir el tamaño de la necesidad de proteger dicho patrimonio. La idea es conocer qué ganan las personas, las empresas y los Estados al tener datos personales de terceros, y la importancia económica de los mismos.

En el presente capítulo se realizará también un estudio sobre la relevancia, respecto de la autorización del titular de los datos personales, sobre el uso de los mismos. En este sentido, por la insuficiencia de la regulación estatal para el tratamiento de datos personales, especialmente en Argentina y Brasil, el consentimiento del titular gana protagonismo en las relaciones privadas, convirtiéndose, quizás, en el principal limitador de la actuación de terceros en la esfera íntima y privada de una persona, en tiempos de revolución tecnológica.

Finalmente, en este capítulo también se realizará una investigación sobre el comportamiento de las empresas propietarias de las redes sociales más utilizadas en Argentina y Brasil. El objetivo es comprender el comportamiento ante el carácter incompleto de las normas estatales sobre protección de datos personales en ambos países.

El estudio se centrará en las políticas para el almacenamiento y tratamiento de datos personales en las redes sociales *YouTube*, *Facebook*, *WhatsApp* e *Instagram*. La elección se realizó en base al informe Digital in 2020 de las agencias de marketing digital, especializadas en redes sociales, We Are Social y Hootsuite, que señalan las redes sociales más utilizadas en el mundo, en enero y julio de 2020.

Con ello se hace una preparación para afrontar el problema central de esta tesis. Antes de abordar la importancia de la necesidad de protección legal de los datos personales de las personas fallecidas, es necesario demostrar que este material tiene su valor económico y patrimonial. En consecuencia, existe una repercusión considerable en el ámbito jurídico del individuo, lo que exige la normatividad que, hasta ahora, no ha sido realizada por Argentina y Brasil, como ha sido demostrado en el capítulo anterior.

2 El valor de los datos personales

En una investigación realizada por la Agencia de Acceso a la Información Pública de Argentina (2019), el Gobierno de dicho país quiso saber cuánto saben sus ciudadanos sobre los derechos de protección de datos personales. El trabajo (mayo de 2019), titulado “Cuánto sabemos de datos personales”, cuestionó, entre otros aspectos, si el entrevistado conocía el derecho a la protección de datos personales. Sobre un total de 4.400 encuestados, 40,5% de las personas afirmaron no conocer tal derecho, un 33,8% sostuvo que sí lo conocía, y el 25,7% restante no supo responder a la pregunta en cuestión.

Se observa que la mayoría de los entrevistados desconocen las normas de protección de datos personales, lo que puede evidenciar un cierto desinterés, o negligencia, del ciudadano común, sobre ello. El resultado también puede reflejar la falta de conocimiento de las personas sobre el valor que estos tienen.

Según Ferrero y Schutz (2018, p. 61) el ciudadano común está lejos de llegar siquiera a imaginar el valor que tienen sus datos, la multiplicidad de modos en que son manipulados, ni tampoco quienes tienen acceso a los mismos y con qué fines

o intenciones. Por lo tanto, es necesario un análisis más profundo de la incorporación de valor económico o patrimonial a los datos personales.

De acuerdo con Fernández (2019, p. 65) una gran parte de la población mundial tiene en su bolsillo o cartera un dispositivo que permite no solo ubicarlos en tiempo real y saber muchísimo acerca de sus conductas y preferencias, sino también reconstruir históricamente esta información en distintos momentos. Además, existe una clara tendencia al aumento en la cantidad y la precisión de la información recolectada, lo que hace que todos estemos virtualmente ubicados en tiempo y espacio durante la mayor parte del día.

Generados por identidades y comportamientos, por individuos y sus acciones en redes digitales, los datos personales son la moneda que se paga por el uso gratuito de plataformas, sitios *web* y servicios *on-line*. Los datos personales se han convertido en un activo económico importante (Silveira; Avelino; Souza; 2016, p. 219).

Según Kahansky (2019, p.12) los datos personales son bienes inmateriales que tienen un papel esencial en la protección de la dignidad del ser humano y de otros valores igualmente fundamentales, pero a la vez tienen un alto valor económico para terceros y se pueden comunicar ilimitadamente sin que ninguno de los sujetos que los ha tenido bajo su dominio lo pierda. En otras palabras, estos bienes personalísimos pueden en cierto sentido desprenderse de su titular y tener vida propia. A pesar de la presencia relevante de archivos físicos, una gran parte de esa vida propia se desarrolla en un espacio que no está ligado a ningún territorio: el ciberespacio.

El mercado de datos personales es cada vez más relevante en la sociedad de la información y puede entenderse como las interacciones económicas encaminadas a la compra y venta de información relacionada con una persona identificada o identificable, directa o indirectamente (Silveira; Avelino; Souza; 2016, p. 220).

Actualmente, los datos personales cuentan con un valor económico, equiparable a ciertos activos intangibles, por ejemplo, el software o el valor comercial de los nombres de dominio. Esto ha llevado a considerarlos el petróleo

de la sociedad de la información y del conocimiento. Aunado a lo anterior, se debe decir que el valor económico otorgado a la información de las personas no radica en el dato por sí mismo, sino en el tratamiento, asociación con otros datos y utilidad que se le dé. Esto permite obtener un lucro, a través de la explotación comercial de aspectos privados, orientados al consumo, que incluso se interesan en predecir conductas y patrones de comportamiento (Enríquez, 2018).

Aún para Enríquez (2018), se puede decir que, en la economía digital, la información se ha convertido en moneda de cambio: ha adquirido un valor elevado y permite que distintos modelos de negocio tengan su sustento en la misma. En este mismo sentido, Henrÿ (2017, p. 112) afirma que se enajenan de esos datos al utilizar todo tipo de aparatos electrónicos interconectados y conectados a Internet. Esos datos sirven para crear riqueza; son medios de producción. Entonces, los individuos no solo contribuyen a la creación de riqueza al trabajar, sino también al proveer datos a aquellos que detenten el poder tecnológico de procesar esos datos y transformarlos en valor económico.

Argumentan Ferrero y Schutz (2018, p. 72) que el problema no sólo yace en la actitud asumida por las empresas que buscan obtener lucro sin respetar límites, sacando frutos a los vacíos legislativos reinantes; sino en la falta de toma de conciencia real por parte de los usuarios del valor que tienen sus datos personales en la sociedad actual.

Para Masili (2018, p. 80) los usos de datos personales para actividades de mercado van más allá del *marketing* y ni siquiera pueden ser rechazados en un papel exhaustivo, principalmente porque, con las tecnologías de big data, la única limitación a la creación de innovaciones en el mercado basado en datos personales es la creatividad.

Ferrero y Schutz (2018, p. 55) también advierten, que los “Datos Personales” se han convertido en un “activo más” que cotiza a un alto valor en el mercado, cuya transmisión y comercialización opera preferentemente a través de Internet, dando origen a un incipiente y acaudalado negocio en torno a ellos: “El Tráfico de Datos Personales”.

Sobre esto, afirma Cejudo (2020, párr. 4) aunque no existan cifras oficiales que den a conocer el valor exacto de todos los datos personales que circulan por Internet, sí hay investigaciones que han sacado a la luz que los perfiles que incluyan los datos financieros, con sus accesos a *PayPal* y *Amazon*, y los propios datos de sus perfiles en las diferentes redes sociales, se venden en el mercado negro por 870 euros.

Por lo tanto, no se puede negar que los datos personales tienen un valor económico y deben incorporarse a sus activos. De hecho, también es innegable que exigen protección jurídica en todas las situaciones. El gran problema es que todavía no existe una definición oficial de valor de los datos personales. Hay afirmaciones abstractas de que los datos tienen valor, pero sin ninguna certeza científica sobre cuánto le cuestan a su comprador. Para algunos, esta herencia es importante. Para otros, tiene un valor irrelevante.

Para Domínguez (2016, p. 15) el dato es un material de valor escaso o nulo para un individuo en una situación concreta, es una representación simbólica que por sí misma no reduce la dosis de ignorancia o el grado de incertidumbre de quien tiene que tomar una decisión. Complementa Domínguez (2016, p. 17), diciendo que la información contenida en los bancos de datos cobra día a día un creciente valor político y comercial. La información se compra y se vende, viaja de un lugar a otro sin que el interesado lo sepa.

No es solo hoy que se intenta identificar el valor que incorporan los datos personales. En 2013, el periódico británico Financial Times creó una calculadora de valor de datos personales. La herramienta se lanzó con la promesa de verificar cuánto puede pagar la industria multimillonaria de corredores de datos por los datos personales de un individuo.

Según Cadman, Freese, Locke y Steel (2013, párr. 3), en la calculadora, los datos de la persona suelen venderse, en promedio, por menos de un dólar. La información general sobre una persona, la edad, el sexo y la ubicación, vale solo $ 0,0005 por persona o $ 0,50 por cada 1000 personas. Una persona que está comprando un automóvil, un producto financiero o unas vacaciones es un poco más valiosa para las empresas que quieren vender estos productos.

Realizando el cálculo durante la producción de este trabajo de doctorado, se pudo constatar que cuánto más ítems relacionados con los intereses del consumidor se seleccionan en la calculadora de datos personales, mayor es el valor asignado. A modo de ejemplo, el valor de los datos personales obtenidos a través de la información proporcionada por el autor de este trabajo fue de US $ 0,7852.

Aún en 2013, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) publicó el estudio *"Exploring the Economics of Personal Data"*, que tenía el objetivo de comprender diferentes metodologías para medir el valor monetario de los datos personales.

El estudio, aunque no concluyente, señaló que hay una falta de datos robustos que puedan analizarse para comprender mejor el valor económico y social de los datos personales. También indicó que las empresas de la cadena deben tener una visión estratégica del valor económico de los datos personales. Y sugirió que, para analizar mejor el valor económico de los datos personales, serían necesarias evaluaciones en contextos regionales de países.

La cuantificación del valor económico de los datos personales también se analizó en el estudio titulado *“What’s Your Data Worth?”*. Short y Todd (2017, p. 17), autores del estudio, hicieron el promedio aritmético del monto pagado por la empresa estadounidense Microsoft en la adquisición de Linkedin y concluyeron que la empresa adquirente pagaba alrededor de US$ 260 por usuario activo mensual.

Los autores citados (2017, p. 19) coincidieron que, aunque las frases "activos digitales" o "activos de datos" se usan comúnmente, no existe una definición aceptada de como estos activos deben contabilizarse en los balances. Para los autores del estudio, de hecho, los activos de datos suelen estar mezclados con otros activos intangibles, como marcas comerciales, patentes, derechos de autor y la capacidad de generar beneficios. Y, cuando se trata de activos intangibles, existen varios enfoques para evaluarlos. Por ejemplo, los activos intangibles pueden valorarse con base en transacciones observables basadas en el mercado que involucran activos similares; sobre los ingresos que producen o el flujo de caja

que generan a través del ahorro; o el costo incurrido para desarrollarlos o reemplazarlos.

Por otro lado, también sugieren Short y Todd (2017, p. 18), al evaluar los datos, que se deben considerar tres fuentes de valor: (1) el valor del activo o acción; (2) el valor de la actividad; y (3) el valor esperado en el futuro.

Aneja y Shapiro (2019), analizando las ganancias que tienen las corporaciones estadounidenses con los datos personales, sugirieron:

> [S]i estamos de acuerdo con la mayoría de los estadounidenses en que cada uno de nosotros posee nuestros propios datos, los estadounidenses deberían recibir una parte sustancial de esos ingresos, ya sea a través de pagos o para financiar objetivos públicos amplios. Con una división de ganancias de 50 a 50, derivada de solo cuatro áreas de información personal de las personas, cada estadounidense que usa Internet recibiría $ 183 en 2020 y $ 308 en 2022. (p. 21).

Lo cierto es que no existe certeza científica sobre el valor económico y patrimonial de los datos personales. Lo que se percibe es que lo menos controvertido es la afirmación de que los datos personales son activos intangibles de difícil valoración. Existen varias posibilidades para cuantificar el valor de los datos personales, lo que dificulta la aproximación del valor de mercado.

Es cierto que las empresas que se ocupan directamente del tratamiento de datos personales cuentan, según lo sugiere la OCDE, con más informaciones y mecanismos de cuantificación de datos personales, ya que incorporan estos bienes en sus activos y en sus operaciones de mercado.

Ejemplificando tales operaciones de mercado, Silveira, Avelino y Souza (2016, p. 221) explican que las muestras comercializadas por empresas como *Google* y *Facebook* resultan del tratamiento de datos extraídos de las acciones de las personas que se recogen en sus bases de datos. Cada individuo recibe un número de identificación (ID) que brinda a estas empresas la posibilidad de atender agencias de publicidad o directamente a los interesados en construir “audiencias” para ofrecer anuncios, promociones, propuestas de servicios, etc. Para obtener datos personales, las corporaciones no cobran por sus servicios, sus ingresos se derivan fundamentalmente de la venta de publicidad dirigida.

No es de extrañar que *Google* y *Facebook* se encuentren entre las de más rápido crecimiento en el mundo en los últimos años. Para Silveira, Avelino y Souza (2016, p. 228) el mercado de datos personales ya es la principal fuente de ingresos para algunas de las grandes corporaciones de la economía de la información. También se ha vuelto imprescindible segmentar la publicidad y organizar muestras de consumidores en audiencias más dispuestas a consumir determinados productos y servicios.

Hemos dicho (Rodovalho, 2021, p. 68) que a lo largo de los años, las empresas que dominaban la mayor cantidad de información de sus clientes y usuarios tenían en este poderoso contenido uno de los principales motores de crecimiento. Y la información transformada en datos se ha convertido en el combustible económico más poderoso de la actualidad.

La confirmación de estas aseveraciones se puede ver en el *ranking* de empresas que más crecieron en 2020, según *Brand Finance*, una consultora de evaluación de negocios de marcas acreditadas e independientes. De acuerdo con la *Brand Finance*, las diez empresas que más hicieron crecer sus marcas hasta junio de 2020 fueron: *Amazon* (1ra.), seguida por *Google*; *Apple*; *Microsoft*; *Samsung Group*; *ICBC*; *Facebook*; *Walmart*; *Ping An* y *Huawei*. El *ranking* continúa mostrando el crecimiento de empresas en el mundo hasta la posición 500. (Rodovalho, 2021, p. 68).

Se nota que la visión sobre el valor de la base de datos para las corporaciones lleva un largo tiempo; no obstante, lo que hace de Internet algo tan discutido hoy en las corporaciones, especialmente por áreas de marketing, son sus características únicas de público objetivo en tiempo real, que permite que las actividades relacionadas con el *marketing* en sí, ventas, distribución y soporte, sean ampliamente exploradas y dirigidas específicamente a un grupo, del cual todas las características se conocen de antemano. De esta forma, puede hacer que las acciones sean más efectivas y, en consecuencia, lograr el objetivo marcado por las empresas (Silveira; Avelino; Souza, 2016, p. 227).

Por otro lado, no solo para el *marketing* los datos de los usuarios ganan valor. De hecho, a través de algoritmos y mecanismos de inteligencia artificial,

estos datos se convierten en todo tipo de información y, a partir de ellos, se toman importantes decisiones, de manera que los algoritmos y otros mecanismos de inteligencia artificial se transforman en oráculos de esta sociedad tecnológica (Masili, 2018, p. 78). No solo las empresas utilizan estas nuevas tecnologías, sino también los responsables de las políticas públicas y de la prestación de servicios públicos (Masili, 2018, p. 89).

Un ejemplo de esto lo traen Mejía y Palmero (2019):

> [E]l uso de datos sanitarios para generar nuevos conocimientos y pruebas sobre la salud a fin de prestar servicios a su población y mejorar los niveles de atención sanitaria es una realidad en muchos países. Además, se está comenzando a compartir esta información entre distintos países con el propósito de maximizar los resultados. Este tipo de análisis se han convertido en un importante insumo para los responsables de la formulación de políticas públicas y se considera que la utilización de estrategias digitales es una estrategia crítica de fortalecimiento de los sistemas de salud para ayudar a alcanzar los Objetivos de Desarrollo Sostenible. (p. 5)

Las actividades más diversas, desde imágenes de cámaras de vigilancia, datos de transacciones económicas, datos personales, hasta búsquedas en *Google*, correos electrónicos y ubicación compartida, generan trazas que pueden matematizarse y procesarse respaldando un volumen exponencial de datos. Las capacidades actuales de captura, almacenamiento y procesamiento han hecho posible un nuevo régimen de visibilidad que ha hecho calculable la totalidad de la vida. Este alcance para administrar el volumen de datos producidos ha introducido un valor de control y previsibilidad con una amplitud y eficiencia sin precedentes para los sectores público y privado. Estas técnicas aparecen como instrumentos para una transformación en la racionalidad de las tácticas gubernamentales (Aragão; Benevides, 2019, p. 2).

La confirmación de esto vino con la pandemia de COVID-19. Explican Almeida *et al* (2020, p. 2488), en tiempos de pandemia por COVID-19, debido a la urgente necesidad de responder con rapidez a los retos que plantea la introducción de un nuevo agente etiológico y la peculiaridad de la enfermedad,

trayendo riesgos a la vida y en materia de salud de las personas, se ha requerido el uso de datos personales de diferentes fuentes para explorar cuestiones científicas en base a características poblacionales, datos de laboratorio y hospitalarios, entre otros, siempre que se guíe por una base ética y legal.

Pero eso no es todo. Para varios otros sectores, los datos personales están ganando cada vez más valor. Otro ejemplo de una actividad en la que los datos personales son cada vez más valiosos, son las campañas electorales.

Aclaran Ramírez y Vignau (2019, p. 86), que en la sociedad moderna las elecciones se enmarcan en un contexto en el que la propaganda electoral es individualizada y se recibe en espacios aislados, con base en un análisis altamente detallado sobre el perfil de las personas que la reciben. En algunas ocasiones, los partidos políticos combinan la información obtenida en el padrón electoral con bases de datos o información pública con la finalidad de obtener rasgos distintivos de las personas que les permita dirigir sus anuncios publicitarios.

Aquí vale la pena reflexionar que, mientras los datos personales están ganando cada vez más valor, la intimidad y privacidad se ponen cada vez más en riesgo. Dice Vercelli (2019, p. 67) que el estado actual es de la fragilidad y la peligrosa desprotección del derecho humano a la intimidad-privacidad de las personas y de las poblaciones. La intimidad-privacidad parece valer cada vez menos. Sus interpretaciones jurídicas dominantes son corporativistas y para-legales. La intimidad-privacidad está desapareciendo a manos de la publicidad (es decir, a manos de los modelos de negocios de las corporaciones que venden publicidad/propaganda).

No se puede negar la creciente importancia de los datos personales para los más variados sectores de la sociedad actual. Ya sea en el ámbito público o privado, el interés de las organizaciones por la información de las personas es algo que ya no se puede ocultar. Es este interés que cubre los datos personales de los individuos de los más variados valores, por ejemplo, patrimonial, económico, político.

El gran problema es que, hasta el momento, no hay claridad sobre el valor real de estos activos. El valor político y social no tiene precio, pero el valor

económico es algo que existe y es cuantificable. El problema es que este valor está lejos del conocimiento de los propietarios de la información. En este punto, es necesario mejorar la legislación nacional para garantizar a los titulares de datos personales el acceso a información que les garantice el conocimiento del valor económico real que tienen sus datos.

3 La importancia del consentimiento

En el 2018, el Poder Ejecutivo Nacional envió al Honorable Congreso de la Nación, un Proyecto de Ley, tendiente a establecer un nuevo ordenamiento legal sobre la Protección de los Datos Personales. En su Mensaje (147/2018), destacó la importancia de adaptar la legislación a la realidad de las nuevas tecnologías y a los cambios regulatorios ocurridos en el derecho comparado durante los últimos años; como así también, expresó su preocupación por la privacidad:

> Es innegable que la evolución de la tecnología en los últimos DIECISIETE (17) años, además de haber producido beneficios innegables para el ejercicio de múltiples derechos, ha impactado en la protección de los datos personales con el surgimiento de nuevas vulneraciones al derecho a la privacidad… (párr. 4°).

El documento precisa, que los derechos básicos del titular de los datos personales son los derechos de acceso, rectificación, oposición y supresión. Según el Gobierno argentino (párr. 21°; Mensaje 147/2018), los cuatro derechos básicos que le corresponden al titular de los datos, aun con otras denominaciones o contenidos sensiblemente diferentes, aparecen en la ley vigente y en las regulaciones más actualizadas en la materia.

En el citado Mensaje, y en relación a los derechos de acceso, rectificación, oposición y supresión antes mencionados, el Gobierno argentino (2018) afirmó:

> [R]especto de estos derechos, las novedades más importantes aparecen en el derecho de oposición al tratamiento de datos y en el derecho de supresión de datos personales. Este último derecho engloba lo que en la actualidad se conoce como "derecho al olvido", denominación usualmente utilizada pero que ha traído muchas discusiones teóricas y críticas sobre su

> aplicación en la práctica, dado que una deficiente implementación podría devenir en violaciones a otros derechos fundamentales, como la libertad de expresión o el acceso a la información. De allí que en la propuesta que se somete a consideración, si bien se reconoce este derecho, se ha aclarado especialmente que el derecho de supresión no procede cuando el tratamiento de datos persiga un fin público o sea necesario para ejercer el derecho a la libertad de expresión e información. (párr. 22)

Aunque hay una declaración del Gobierno argentino de que los derechos de oposición y supresión de los datos personales son nuevos, cabe mencionar, que la Ley 25.326, de Protección de los Datos Personales, ya contenía en su texto una disposición expresa sobre el derecho de supresión en el artículo 16, como en otros artículos de la norma en cuestión. Se destaca aquí, que un estudio más profundo sobre el derecho a la supresión y el “Derecho al Olvido”, se realizará en los próximos capítulos, cuando se aborde el instituto de acuerdo con las leyes de la Argentina y Brasil.

En cuanto al derecho de oposición, señalado en el artículo 43, párrafo 3, de la Constitución de la Nación Argentina, de hecho, no existía una disposición expresa para regular el instituto en la Ley 25.326. Con el proyecto antes mencionado de la nueva ley argentina de protección de datos, el derecho de oposición se ha convertido en uno de los puntos de actualización, según lo previsto en el artículo 30:

> [E]l titular de los datos puede oponerse al tratamiento de sus datos, o de una finalidad específica de éste, cuando no haya prestado consentimiento. El responsable del tratamiento debe dejar de tratar los datos personales objeto de oposición, salvo que existan motivos legítimos para el tratamiento que prevalezcan sobre los derechos del titular de los datos. (Mensaje 147/2018).

Explican Bosque y Villan (2018, p. 4), puede oponerse al tratamiento de los datos si se hubiesen recabado sin su consentimiento o cuando existen motivos fundados para ello. Se observa que el derecho de oposición es un arma

importante contra el tratamiento no consentido de datos personales, lo que ya resalta la importancia del consentimiento bajo la nueva ley argentina.

Para Masciotra (2018, pp. 5-6), la elaboración doctrinaria de los principios que rigen el tratamiento de los datos personales plasmados en normas legales otorga un marco de protección a su titular en el que su consentimiento resulta liminar para otorgar legitimidad a todas las operaciones que conforman el tratamiento de datos, sea la recolección, conservación, ordenamiento, almacenamiento, modificación, evaluación, bloqueo, destrucción y cesión a terceros. En este sentido, para Mendes y Fonseca (2020, p. 509), no es exagerado afirmar que el consentimiento ha figurado como instrumento regulador central y núcleo de legitimidad práctica de este régimen protector.

Es que, desde esta perspectiva, este individuo se guía por la maximización de sus intereses frente a los costos y beneficios que implica consentir, o no, con los términos que se le presentan. Así, si dispone de un conocimiento amplio sobre lo que se hace con sus datos personales, puede sopesar los costos que supone para su personalidad y compararlos ante los beneficios que aporta, por ejemplo, al utilizar un servicio *on-line*. Por lo tanto, tomará una decisión sobre qué consentir y qué no consentir en Internet, en su mejor interés**;** por ejemplo, después de leer los términos de privacidad proporcionados (Mendes; Fonseca, 2020, p. 514).

Para Addati (2020), cuando se usa un instrumento virtual de comunicación ofrecido por la red y a través suyo, el sujeto revela información personal. De cierto modo estaría consintiendo la intromisión a su esfera privada y al uso de la información así obtenida por un tercero. Sin embargo, ese consentimiento -como vimos- es revocable en cualquier momento, decisión que debería imponerse sobre los terceros que hayan accedido a esa información impidiéndoles su uso. Es aquí donde entra en juego el derecho a la protección de los datos personales como el instrumento jurídico que apodera al sujeto para seguir manteniendo un poder de control sobre el uso y destino de esa información (p. 59).

La importancia que se le da al consentimiento en el sistema argentino de protección de datos ya estaba reflejada en el artículo 5 de la Ley 25.326, que disponía que el tratamiento de datos personales es ilícito cuando el titular no

hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias. Ya en el proyecto de la nueva ley, el consentimiento se ha regulado principalmente en los artículos 12, 13 y 14, adquiriendo contornos aún más importantes que los traídos en la legislación anterior.

Explica Juri (2019, p. 226), que la regulación que propone el proyecto es más acorde con el concepto correspondiente al estado de desarrollo conocido como “la era digital” y con las nuevas tecnologías. Ciertamente el consentimiento sigue siendo uno de los principios rectores para el tratamiento de datos personales, pero la propuesta incluye parámetros que admiten otorgarlo, de manera más clara, sin que ello impida la innovación y el avance de nuevas tecnologías y usos en Internet.

Por otro lado, también se ve que, si bien existe una centralidad del consentimiento en el sistema de protección de datos argentino, no hay exclusividad. El tratamiento de datos personales sin la autorización del titular está exceptuado en el artículo 11 del proyecto de la ley argentina de protección de datos, en los siguientes casos:

> [A]rtículo 11.- Licitud del tratamiento de datos. El tratamiento de datos es lícito sólo si se cumple al menos UNA (1) de las siguientes condiciones:
> a. El titular de los datos dé su consentimiento para el tratamiento de sus datos para uno o varios fines específicos conforme lo dispuesto en los artículos 12, 13 y 14 de la presente;
> b. El tratamiento de datos se realice sobre datos que figuren en fuentes de acceso público irrestricto;
> c. El tratamiento de datos se realice en ejercicio de funciones propias de los poderes del Estado y sean necesarios para el cumplimiento estricto de sus competencias;
> d. El tratamiento de datos sea necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
> e. El tratamiento de datos derive de una relación jurídica entre el titular de los datos y el responsable del tratamiento, y resulte necesario para su desarrollo o cumplimiento;

> f. El tratamiento de datos resulte necesario para salvaguardar el interés vital del titular de los datos o de terceros, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos del titular de los datos, y el titular de los datos esté física o jurídicamente incapacitado para dar su consentimiento;
> g. El tratamiento de datos sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos del titular de los datos, en particular cuando el titular sea un niño, niña o adolescente. (Mensaje 147/2018).

La ley brasileña no es diferente. El consentimiento tomó protagonismo en las situaciones que autorizaban el tratamiento de datos personales con la llegada de la Ley 13.709/2018, LGPD. De acuerdo con lo dispuesto en el artículo 8 de la ley, el consentimiento en Brasil siempre debe darse por escrito o por otro medio que demuestre la manifestación de la voluntad del titular, libre de cualquier defecto en el consentimiento, con nulas autorizaciones genéricas.

Explican Bosque y Villan (2018, p. 3) que la ley brasileña propone que la misma sea aplicable a empresas que tienen sede en dicho país y realicen recolección de datos en su territorio. Además de requerirse el consentimiento del ciudadano para el tratamiento de los datos, también se deben brindar las herramientas para que el usuario de los datos pueda acceder, corregir o eliminar toda la información.

La LGPD no exige que el consentimiento se brinde únicamente por escrito**,** como se puede observar en el artículo 8º, que dispone**,** que “El consentimiento previsto en el inciso I del artículo 7 de esta Ley deberá ser aportado por escrito o por cualquier otro medio que demuestre la intención del titular”. […] Sin embargo, la expresión de voluntad debe ser inequívoca, según el artículo 5, XII, de la LGPD, que sigue el mismo entendimiento del RGPD europeo, cuyo artículo 11 deja claro que la voluntad debe ser explícita, entendiéndose así la voluntad traducida en una declaración o acto positivo inequívoco (Frazão, 2018, párr. 6-7).

Al igual que en el sistema argentino, en Brasil, el consentimiento, aunque también es el principal medio para autorizar el procesamiento de datos

personales, no es el único. El artículo 7 de la LGPD regula cuáles son las situaciones que permiten el tratamiento:

> [A]rtículo. 7 ° El tratamiento de datos personales solo podrá realizarse en los siguientes casos:
> I - dando el consentimiento del titular;
> II - para el cumplimiento de una obligación legal o reglamentaria por parte del responsable del tratamiento;
> III - por la administración pública, para el tratamiento y uso compartido de los datos necesarios para la ejecución de las políticas públicas previstas en las leyes y reglamentos o sustentadas en contratos, convenios o instrumentos similares, sujeto a lo dispuesto en el Capítulo IV de esta Ley;
> IV - realizar estudios por un organismo de investigación, garantizando, siempre que sea posible, el anonimato de los datos personales;
> V - cuando sea necesario para la ejecución de un contrato o trámites preliminares relacionados con un contrato en el que el titular sea parte, a solicitud del titular de los datos;
> VI - para el ejercicio regular de derechos en procedimientos judiciales, administrativos o arbitrales, este último en los términos de la Ley N ° 9.307, de 23 de septiembre de 1996 (Ley de Arbitraje);
> VII - para la protección de la vida o seguridad física del titular o tercero;
> VIII - para la protección de la salud, exclusivamente, en un procedimiento realizado por profesionales de la salud, servicios de salud o autoridad sanitaria;
> IX - cuando sea necesario para atender los intereses legítimos del responsable del tratamiento o de un tercero, excepto en el caso de que prevalezcan los derechos y libertades fundamentales del titular que requieran la protección de datos personales; o
> X - para protección crediticia, incluidas las disposiciones de la legislación pertinente.

Se observa que las situaciones que autorizan el procesamiento de datos personales son similares en los dos países, siendo un poco más detallado el legislador brasileño que el legislador argentino, aun cuando se ocupó de legislar sobre el tratamiento de datos personales sensibles. En este punto, el artículo 11 de la LGPD trató de explicar la importancia del consentimiento, por lo que este tipo de autorización es la regla.

La existencia de diferentes formas de autorización para el tratamiento de los datos personales es saludable. Bioni (2019, p. 293) aclara que la autonomía de la voluntad debe ser limitada, asegurando que el flujo de información sea adecuado para el libre desarrollo de la personalidad. Además de los supuestos ya previstos en el ordenamiento jurídico que establecen núcleos duros para el consentimiento del titular, se encontró que la privacidad contextual amplía el horizonte normativo para la solución de casos en los que el consentimiento ocasionaría distorsiones al valor social de la protección de datos personales.

Cabe destacar que el consentimiento no es una innovación que traen las leyes de protección de datos de Argentina y Brasil. Se mencionó en el ítem 3 del Capítulo II, que, en 1990, ya existían en el Código Brasileño de Protección al Consumidor, vestigios de la necesidad del consentimiento para el procesamiento de datos personales.

El párrafo 3 del artículo 43 del citado Código dispone, desde la publicación de la ley respectiva que el consumidor, cuando encuentre inexactitud en sus datos y registros, podrá exigir su inmediata corrección, debiendo el archivero, dentro de los cinco días comunicar el cambio a los destinatarios de la información incorrecta. El artículo analizado, trata sobre la posibilidad de crear bases de datos y registros de consumidores. Estas bases de datos, aunque independientes del consentimiento del consumidor para la inclusión de sus datos, deben respetar la autonomía de la voluntad a la hora de solicitar su corrección.

Cabe señalar que el Código Brasileño de Defensa del Consumidor surge en el contexto de la llamada segunda generación de leyes de protección de datos personales, cuando la necesidad de consentimiento para el procesamiento de datos personales ya existía, pero aún no se había vuelto esencial.

Para Bioni (2019, p. 171), la segunda generación de leyes de protección de datos personales se caracteriza por un cambio en el núcleo regulatorio. No solo se ocupa de las bases de datos estatales, sino también de las del ámbito privado. La figura del Gran Hermano (una base de datos única y centralizada) se diluye por la de Hermanitos (bases de datos dispersos en el Estado y plan privado).

También, según Bioni (2019, p. 171), la segunda generación de leyes transfiere la responsabilidad de protegerlas al propio interesado. Si antes el flujo de información personal debió haber sido autorizado por el Estado, ahora le corresponde al propio ciudadano intervenir, mediante consentimiento, para establecer sus opciones en cuanto a la recopilación, uso y puesta en común de sus datos personales.

Igualmente, el consentimiento pleno como medio para autorizar el procesamiento de datos solo ocurrió en la próxima generación de leyes de procesamiento de datos personales. Explica Bioni (2019, p 172), que en esta etapa, las normas para la protección de los datos personales buscaban asegurar la participación del individuo en todos los movimientos de sus datos personales: desde la recogida hasta el intercambio. De esta manera, se lograría el éxtasis de la terminología de “autodeterminación informativa”, porque con esa participación, el sujeto podría tener un control más amplio sobre su información personal.

Han surgido diferentes bases legales para el procesamiento de datos, ya en el contexto de la actual cuarta generación de leyes de procesamiento de datos personales. Bioni concluye (2019, p. 173) señalando que este avance generacional no ha eliminado el papel del consentimiento. Su centralidad siguió siendo el sello distintivo del enfoque regulador. Tanto es así que, en medio de este proceso evolutivo, el consentimiento pasó a ser adjetivo, ya que debía ser libre, informado, inequívoco, explícito y/o específico, igual a lo que ocurre en el derecho comunitario europeo.

Argentina y Brasil se inspiraron en el derecho europeo, para actualizar su legislación sobre el procesamiento de datos personales. De ahí la continuidad del protagonismo del consentimiento. Es posible notar la similitud entre las disposiciones legales nacionales de los dos países con la normatividad traída en el artículo 4.11 del Reglamento General de Protección de Datos (Europa, 2016), que define el consentimiento como toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

Siguiendo el ejemplo del Reglamento Europeo, las leyes de Argentina y Brasil incorporan varios mecanismos que tienen por objeto asegurar que el consentimiento se otorgue con la debida libertad y sin ninguna adicción.

El protagonismo y la necesidad de un consentimiento libre, específico, informado e inequívoco se ilustra en el considerando 32 del Reglamento Europeo, cuya idea se refleja en los sistemas argentino y brasileño de protección de datos personales:

> [E]l consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio *web* en Internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta.

Bosque y Villan (2018, p. 7) advierten que, una vez obtenida la información, las empresas y los responsables de bases de datos pueden usar la información que recopilan, con previo consentimiento por parte del usuario, sólo para los propósitos específicos, explícitos y legítimos. No pueden utilizarla con otro propósito que aquel para la cual fue recopilada, transferida o compartida. En el caso que deseen hacerlo, deberá realizarse con el consentimiento del usuario.

De lo aquí expuesto se puede extraer que el protagonismo del consentimiento en el tratamiento de datos personales tiene su razón de existir en

un patrimonio jurídico mayor que la protección de los datos en sí. La autodeterminación informativa, de la que tanto se habló en el ámbito de la protección de datos personales, termina siendo sólo una herramienta para la protección de la intimidad, la privacidad y la libertad del individuo y, en consecuencia, la dignidad de la persona humana. De ahí la importancia que se le da al consentimiento, ya que es una barrera eficaz contra los ataques indebidos a los datos personales y protege los derechos citados.

Por otro lado, se vio que el camino por el cual la legislación de protección de datos personales ha ido evolucionando, especialmente en la segunda y tercera generación de leyes, llevaría el consentimiento al nivel de los únicos medios admisibles de autorización para su tratamiento.

Este camino resultó inadecuado, ya que el aislamiento de los datos de las personas, con acceso, exclusivamente, a través del consentimiento traería una serie de complicaciones en los más variados sectores. Por esta razón, la legislación contemporánea, basada en el Reglamento Europeo de Protección de Datos Personales, al igual que las leyes de Argentina y Brasil, ha permitido el acceso a los datos personales por medio de diferentes fuentes, sin autorizar ningún protagonismo entre ellas.

Asimismo, sostiene Faliero (2018, p. 70) que no se debe perder en vista que el examen de la legislación tiene por objeto la tutela de un sujeto vulnerable, el titular del dato, que se encuentra en condiciones desiguales frente a su contraparte, el responsable del tratamiento. Su desigualdad se funda en los mismos extremos que los que comparte con otro débil jurídico, el usuario o consumidor, por su debilidad económica, estructural e informativa.

4 Las políticas de privacidad y almacenamiento de datos en las redes sociales más utilizadas en Argentina y Brasil

El crecimiento exponencial de las redes sociales en todo el planeta es innegable y el poder de integración de estos mecanismos se puede ejemplificar a través de la teoría de los seis grados. Afirma, Molina Quiroga (2017), que de

acuerdo con la teoría de los seis grados de separación cada persona conoce en promedio entre amigos, familiares y compañeros de trabajo o escuela unas 100 personas. Entonces si cada una de ellas conoce a otras 100 personas, cualquier individuo puede pasar un recado a 10.000 personas tan sólo en el primer grado, en ese estado imagina que al llegar al sexto nivel y con las tecnologías disponibles a través de las redes sociales, podría hacerse llegar un mensaje a cualquier individuo del planeta (pp. 3-4).

Según el informe *Digital in 2020* antes mencionado de las agencias de *marketing* digital, especializadas en redes sociales, *We Are Social* y *Hootsuite*, que enumera las redes sociales más utilizadas en el mundo, para enero de 2020, cerca de 3.800 millones de personas utilizaban las redes sociales en el mundo; incrementándose dicho número, a julio de 2020, en 3.960 millones, logrando con ello, que más de la mitad de la población mundial se convirtiera en usuarios de las redes sociales. Al enero de 2021, de acuerdo con el informe Digital in 2021 de las mismas agencias (Kemp, 2021a, párr. 8), este número ya era de 4.200 millones de usuarios – 53% de la población mundial.

Para Kemp (2020a, párr. 4), el marco de 2020 es aún más impresionante si se considera que la mayoría de las empresas de redes sociales restringen el uso de sus plataformas para personas menores de 13 años. De hecho, las últimas cifras indican que casi dos tercios (65%) de la población 'elegible' total del mundo ahora usan las redes sociales.

Según Kemp (2020b, p. 43) existían en la Argentina, a enero de 2020, 34 millones de usuarios activos de redes sociales (informe *Digital 2020: Argentina*). Al mes enero de 2021, de acuerdo con Kemp (2021b, p. 47) este número ya era de 36 millones (informe Digital 2021: Argentina). Considerando a los usuarios de Internet entre 14 y 64 años, las redes sociales más utilizadas hasta enero de 2021 fueron: YouTube (95,8%); WhatsApp (92,9%); Facebook (90,4%); e Instagram (85,3%).

En Brasil, el informe *Digital 2020: Brazil* (Kemp, 2020c, p. 43) contabilizaba 140 millones de usuarios de redes sociales en dicho país al mes de enero de 2020. Al enero de 2021, según el informe *Digital 2021: Brazil* (Kemp, 2021c, p.

47), eran 150 millones de usuarios. Considerando el mismo grupo de edad de usuarios mencionado anteriormente, las redes sociales más utilizadas fueron: *YouTube* (96,4%); *WhatsApp* (91,7%); *Facebook* (89,8%) e *Instagram* (86,3%).

Kemp (2020d, párr. 1-2) explica que el panorama digital global ha evolucionado rápidamente en la segunda mitad de 2020, con la pandemia de Coronavirus en curso, la que continúa influyendo y remodelando varios aspectos de nuestra vida cotidiana. Las cuarentenas pueden haber sido levantadas en algunos países, pero los nuevos comportamientos digitales adoptados durante el confinamiento perduran, redundando en el crecimiento de las actividades digitales y el universo *on-line*.

Queda claro, que el cambio en el comportamiento social y digital de las personas, ya se estaba intensificando antes de la pandemia de coronavirus. En este aspecto, explica Schwab (2016, p. 20), que las tecnologías digitales, basadas en computadoras, software y redes, si bien no son nuevas, están causando disrupciones en la tercera revolución industrial, al volverse más sofisticadas e integradas; transformando, en consecuencia, la sociedad y la economía global.

Complemento Assunção y Matos (2014, p. 540) señalan que las redes sociales *on-line* han cambiado la naturaleza de las relaciones entre las personas, y desde su aparición, han atraído a millones de usuarios, que las han integrado a su vida diaria.

El avance de las redes sociales en la vida de las personas, y aquello que sucede con las tecnologías digitales y sociales, trae problemas nunca antes experimentados. Ejemplifica Schwab (2016, p. 89), que, si bien los canales digitales ofrecen oportunidades para la difusión de información y la organización de iniciativas para buenas causas, también pueden utilizarse para difundir contenidos malignos, propaganda y, como en el caso de ISIS, utilizado por grupos extremistas, para reclutar y movilizar seguidores. Los adultos jóvenes son particularmente vulnerables, especialmente cuando no tienen una red de apoyo social estable.

La idea inicial de la tecnología era enriquecer la personalidad, ampliando sus conocimientos y su capacidad para dominar las cosas que lo rodeaban,

brindándole mayor comodidad. Este es también el caso desde que se ha incrementado la protección de la salud, la seguridad del transporte y de las casas, se han desarrollado nuevos puestos de trabajo y se ha facilitado la comunicación y el acceso a la información; pero ese propósito se ha desviado desde el momento en que se ha convertido más en un producto de consumo que en algo beneficioso, y la forma en que las personas lo han usado a menudo ha sacrificado sus propias personalidades al facilitar la intrusión en la información y momentos particulares de sus vidas (Creste; Tebar, 2017, p. 4).

En este sentido, advierte Schwab (2016, p. 133) las preocupaciones de los ciudadanos, en cuanto a la privacidad y el establecimiento de la responsabilidad comercial y en las estructuras legales, requerirán ajustes en la forma de pensamiento y pautas para el uso y prevención del perfil individual de las personas (*profiling*), y sus imprevistas consecuencias.

La presencia en el mundo digital ha evolucionado rápidamente en los últimos 20 años o más. Hace apenas 10 años, eso significaba tener un número de teléfono celular, una dirección de correo electrónico y quizás un sitio *web* personal o una página de MySpace. Ahora, la presencia digital de las personas se lleva a cabo por medio de sus interacciones digitales y rastros a través de una multitud de plataformas *on-line* y medios de comunicación. Varias personas tienen más de una presencia digital, una página de *Facebook*, una cuenta de *Twitter*, un perfil de *Linkedin*, un blog en *Tumblr*, una cuenta de *Instagram* y, a veces, más que eso (Schwab, 2016, p. 115).

En nuestro mundo cada vez más conectado, la vida digital tiende a asociarse estrechamente con la vida personal. En el futuro, desarrollar y gestionar una presencia digital será tan común como cuando las personas decidan sobre presentarse al mundo todos los días a través de la moda, las palabras y los hechos. En este mundo conectado y a través de su presencia digital, las personas podrán buscar y compartir información, expresar libremente sus ideas, encontrar y ser encontrado y desarrollar y mantener relaciones prácticamente en cualquier parte del mundo (Schwab, 2016, pp. 115-116).

Desde el momento en que el ser humano se virtualiza en el mundo digital, con el desarrollo de la tecnología, su personalidad, en ambos aspectos, sigue inexorablemente este desenrollar. La persona utiliza su personalidad jurídica para, por ejemplo, celebrar varios contratos *on-line*. Asimismo, se discute cada vez más la protección de sus atributos intrínsecos de red, por ejemplo, la imagen y el honor. No será descabellado defender, en un futuro próximo, la existencia de una personalidad virtual, condensadora de la personalidad jurídica y los derechos de la personalidad, cuando se proyecte en el universo digital (Zampier, 2021, pp. 102-103)

Schwab (2016, p. 76) afirma que la agregación de significativas bases de datos está permitiendo a los grandes operadores on-line deducir más información que la proporcionada (implícita o explícitamente) por los usuarios. La caracterización de los perfiles de los usuarios a través del análisis de importantes volúmenes de datos e inferencias técnicas está allanando el camino para nuevos servicios, más personalizados y adaptados, que pueden beneficiar a usuarios y consumidores, pero que también generan preocupación en materia de privacidad del usuario y de la autonomía individual.

Para Zampier (2021, p. 22), la identidad digital se nutre de los contenidos que suben a la gran red mundial de computadores. Parte de este contenido está disponible por los propios sujetos; otra parte la cargan terceros que muchas veces ni siquiera cuentan con la autorización de los titulares. Aún para Zampier (2021, p. 23), alimentando las redes sociales con fotos, opiniones y reportajes del día a día, insertando archivos en las nubes de Internet, interactuando con otros actores sociales a través de sus dispositivos electrónicos, el ser humano del mundo moderno va estableciendo una dependencia cada vez mayor con el entorno virtual.

En este contexto de formación de la personalidad virtual, las redes sociales tienen gran importancia, ya que, en gran medida, reciben información de sus usuarios en las situaciones más diversas. Para Farias y Monteiro (2012, p. 10) las elecciones que hace cada usuario para presentarse no como realmente es, sino como podría llegar a ser, teniendo en cuenta aspectos que pueden demostrar lo

que realmente es son componentes de una nueva personalidad. Una personalidad creada para ser ejecutada allí, y solo allí, en el campo cibernético de interacción.

Mientras que las plataformas de las empresas logran agregar datos de sus consumidores solo relacionados con el escenario de compras y búsquedas que allí se realizan, las redes sociales reciben con mayor frecuencia y, a menudo, de forma voluntaria, datos generales, sensibles y de la vida privada. No en vano, las redes sociales ahora se consideran un activo digital con valor económico, integrando así los activos del usuario.

Ejemplifican Barreto y Nery Neto (2016, p. 1), que existe una gran exposición diaria de cada individuo en Internet, con publicación de fotos, imágenes, videos, almacenamiento de contenido en la nube y una infinidad de situaciones que terminan formando un gigantesco patrimonio digital. En algunos casos, las cuentas de redes sociales monetizan valores astronómicos, sumando millones de seguidores. Para los autores en foco (2016, p. 7), en tales casos pueden haber valiosas colecciones digitales (innumerables libros, películas, canciones) adquiridas por el usuario y perfiles de redes sociales que generan ingresos mensuales.

Siendo los principales agregadores de datos personales y, en consecuencia, formando perfiles virtuales que son de gran importancia en la formación de la personalidad virtual de las personas, las redes sociales tienen una enorme responsabilidad en el tratamiento de los datos de sus usuarios. Este procesamiento de datos continúa existiendo después de la muerte del individuo. Para Addati (2020, p. 70) hay una tendencia a la incertidumbre jurídica para los operadores del Derecho, la que debe ir zanjándose en virtud de la cotidianeidad que ha adquirido Internet y las redes sociales en torno a la vida diaria de millones de personas para trabajar, sociabilizar e informarse.

De ahí la relevancia para este trabajo del conocimiento sobre las políticas de almacenamiento de datos personales de las redes sociales. Por lo señalado, y a partir de ahora, se puede comprender la forma por la cual las redes sociales más utilizadas en Argentina y Brasil tratan los datos personales de sus usuarios,

especialmente después de su muerte; aquello que se acerca al problema central del presente trabajo.

La elección de las redes sociales que tendrán sus políticas de tratamiento de datos estudiadas y explicadas, se basaron en el informe *Digital in 2020*, que señala las redes sociales más visitadas en Argentina y Brasil. A partir de este informe se analizarán las políticas de almacenamiento y tratamiento de datos personales en las redes sociales *YouTube*, *Facebook*, *WhatsApp* e *Instagram*.

La primera red social que tiene su política de almacenamiento y tratamiento de datos personales, analizada, es *YouTube*; la plataforma más utilizada en Argentina y Brasil. Silva y Carvalho Júnio (2020, p. 132) dan fe de que *YouTube* es una red social, porque las personas que la utilizan e interactúan dentro de ella son las que mantienen en marcha esta plataforma. Explican Amendola y Carneiro (2019, p. 2), que *YouTube* es una plataforma *on-line* de acceso libre y acceso en el que cualquiera puede crear una cuenta y un canal, y luego vincular vídeos, en formato digital, con derechos de autor o no. Dentro de la plataforma también es posible participar en grupos y suscribirse a canales, priorizando el acceso a la información que estos últimos brindan. También es posible guardar los contenidos o replicarlos en su propio canal.

YouTube pertenece a *Google*, por lo que cuando un usuario hace clic dentro de *YouTube* en "Condiciones de privacidad", se le dirige a una página de la empresa propietaria (https://policies.google.com/privacy?hl=pt-BR&gl=br) y no de la propia red social. Se presenta la política general de privacidad de *Google*, vigente a partir del 30 de septiembre de 2020, donde se justifica la aplicación de dicha política de la siguiente manera:

> [E]sta Política de Privacidad se aplica a todos los servicios ofrecidos por *Google* LLC y sus afiliados, incluidos *Youtube*, *Android* y los servicios ofrecidos en sitios *web* de terceros, como los servicios de publicidad. Esta Política de Privacidad no se aplica a los servicios que tienen políticas de privacidad independientes que no incorporan esta Política de Privacidad. (Google, 2020a, section 10, párr. 1).

Así, al analizar la política de privacidad de *YouTube*, de hecho, se está analizando la política de la empresa propietaria de la red social. En la misma página, *Google* comunica qué información se recopila:

> [R]ecopilamos informaciones para brindar mejores servicios a todos nuestros usuarios, lo que incluye descubrir cosas básicas, como el idioma que habla, cosas aún más complejas, como los anuncios que puede encontrar más útiles, las personas on-line que más importan para ti o los videos de *Youtube* que te pueden gustar. La información recopilada por *Google* y cómo se usa esa información depende de cómo usa nuestros servicios y cómo administra los controles de privacidad. (*Google*, 2020a, section 2, párr. 1).

Aún, respecto a la misma recopilación de datos:

> [C]uando no ha iniciado sesión en una cuenta de *Google*, almacenamos la información que recopilamos con identificadores únicos vinculados al navegador, aplicación o dispositivo que está utilizando. Esto nos ayuda a mantener las preferencias de idioma en todas las sesiones de navegación, por ejemplo. [...] Cuando inicia sesión, también recopilamos información que almacenamos con su cuenta de *Google* y que tratamos como información personal. (*Google*, 2020a, section 2, párr. 2-3).

Y la empresa propietaria de *YouTube* continúa aclarando su recopilación de datos:

> [T]ambién recopilamos contenido que usted crea, carga o recibe de otros cuando usa nuestros servicios. Esto incluye correos electrónicos enviados y recibidos, fotos y videos guardados, documentos y hojas de cálculo creados y comentarios hechos en videos de *Youtube*. (*Google*, 2020a, section 2, párr. 5).

Se nota que, cuando usa *YouTube*, el usuario ofrece más que información sobre sus búsquedas de videos. De hecho, la empresa propietaria recopila información que genera un perfil virtual dotado de lenguaje, comportamiento del consumidor y relaciones personales, entre otros datos. Esto se vuelve aún más claro cuando, en la Política de Privacidad de *YouTube/Google*, se divulgan las siguientes informaciones:

> [R]ecopilamos información sobre su actividad en nuestros servicios y usamos esa información para recomendar un video de *Youtube* que podría gustarle, por ejemplo. La información de la actividad que recopilamos puede incluir lo siguiente: términos que busca; videos que ve; vistas e interacciones con contenido y anuncios; información de voz y audio cuando utiliza funciones de audio; actividad de compra, personas con las que se comunica o comparte contenido; actividades en sitios *web* y aplicaciones de terceros que utilizan nuestros servicios; Historial de navegación de Chrome que sincronizaste con tu cuenta de *Google*. Si utiliza nuestros servicios para realizar y recibir llamadas o enviar y recibir mensajes, podemos recopilar información de registro telefónico, como su número de teléfono, número de llamada, número de llamada, números de reenvío, hora y fecha de las llamadas y mensajes, duración de la llamada, información de enrutamiento y tipos de llamadas. (*Google*, 2020a, section 2, párr. 9-10).

La recopilación de datos es demasiado extensa y va más allá de lo que ya se ha expuesto aquí. Por ejemplo, se recopila información relacionada con el movimiento geográfico del usuario. Según *Google* (2020a, section 2, párr. 12), cuando se utilizan servicios como *YouTube*, se recopila información sobre la ubicación del usuario, ofreciendo películas, indicando los cines más próximos y sus horarios; como así también, sitios para compras, y direcciones para un viaje de fin de semana.

Google (2020a, section 3) justifica dicha recopilación de informaciones, *afirmando* que utiliza los datos personales de los usuarios para proporcionar, mantener, mejorar, desarrollar y personalizar sus servicios. Además, también informa que los datos recopilados se utilizan para la propia evaluación de desempeño y para contactar y proteger a sus usuarios. En cuanto a compartir los datos recopilados, *Google* (2020a, section 5) explica que no comparte información personal con empresas, organizaciones o personas ajenas a *Google*. Las excepciones a esta política son, la de compartir en el caso que el usuario lo autorice; con administradores de dominio; para procesamiento externo por afiliados o empresas asociadas y por razones legales.

La política de privacidad de *YouTube/Google* (2020a, section 5) no prevé la duración del procesamiento de los datos personales de sus usuarios, pero se refiere a la política denominada "Tecnologías". En esta política es posible encontrar información sobre los períodos de almacenamiento de datos. Según *Google* (2020b, section 9, párr. 4), los datos personales del usuario permanecen en la cuenta de *Google* hasta que el usuario elige eliminarlos.

Google (2020b, section 9, párr. 5) explica que, en algunos casos, en lugar de proporcionar una forma de eliminar datos, hay almacenamiento durante un período predeterminado. Así, para cada tipo de datos se definen intervalos de retención en función del motivo de la recogida, que varían, por ejemplo, entre 9 y 18 meses. En ningún momento la Política de Privacidad de *YouTube/Google* explica qué se hará con los datos personales de los usuarios fallecidos. Pero la Compañía no ignora esta posibilidad.

En su página de “Ayuda de la Cuenta de *Google*” (2020c, párr. 4) se presentan algunas posibilidades para el tratamiento de los datos del usuario fallecido. La primera es la voluntad del usuario, previamente manifestada en el mecanismo denominado "Administrador de cuentas inactivas", donde puede informar quién debe tener acceso a su información y si quiere que su cuenta sea eliminada. Pero *Google* (2020c, párr. 3) reconoce que gran parte de las personas mueren sin dejar instrucciones claras sobre la administración de sus cuentas *on-line*. Por lo tanto, se presentan las siguientes posibilidades:

> [P]odemos trabajar con familiares directos y representantes para cerrar la cuenta de una persona fallecida, cuando sea apropiado. En determinadas circunstancias, podemos proporcionar el contenido de la cuenta de un usuario fallecido. En todos estos casos, nuestra responsabilidad principal es mantener la información de las personas segura, protegida y privada. No podemos proporcionar contraseñas u otros detalles de inicio de sesión. Cualquier decisión de responder a una solicitud sobre un usuario fallecido solo se tomará después de una cuidadosa consideración (*Google*, 2020c, párr. 3).

Se advierte que la Compañía no tiene clara la forma de acceder y transferir los datos del usuario fallecido, dejando bajo su subjetividad la decisión de

proporcionar la información a terceros o no. *Google* (2020c, párr. 3) no descarta la posibilidad de proporcionar el contenido de la cuenta de un usuario fallecido, lo que pone en riesgo la intimidad y privacidad *post mortem*. Un formulario de solicitud para acceder al contenido de la cuenta de un usuario fallecido es ofrecido por *Google* a la parte interesada.

El interesado debe completar el formulario, aceptando la condición de que, si se aprueba la solicitud, deberá tener un instrumento de garantía, con texto proporcionado por *Google*, que se emita en los Estados Unidos. Además, deberá presentar, junto con la solicitud, documentos de la identificación oficial del solicitante y el certificado de defunción del usuario, los cuales deben estar en inglés o con una traducción al inglés certificada por un profesional jurado.

La segunda red social analizada, que tiene su política de privacidad y de datos personales, es *Facebook*. Para Ponte (2020, p. 3) *Facebook* es una de las redes sociales más utilizadas a nivel mundial y cuyo principal objetivo es acercar a las personas, independientemente de su ubicación, edad, profesión o género. Esta red en particular permite y fue diseñada para que todos puedan tener voz y ser escuchados, incluso cuando contradigan los derechos de los demás; conectar, unir y crear una comunidad; servir a todos con tecnología accesible; proteger a las personas y su intimidad-privacidad, y promoción de oportunidades económicas.

A diferencia de *YouTube*, *Facebook* tiene su propia política de privacidad y tratamiento de datos personales, que se denominó “Política de Datos”. A partir del 10 de octubre de 2020, fecha de la consulta, la política de privacidad y tratamiento de datos de la Red Social brinda información sobre la recolección, uso, intercambio, control y eliminación de los datos personales de sus usuarios, entre otros. Al igual que *YouTube/Google*, *Facebook* recopila casi cualquier cosa relacionada con el usuario a su alcance. En la página de Política de Datos, *Facebook* (2020a) deja claro:

> Recopilamos el contenido, las comunicaciones y otras informaciones que usted proporciona cuando utiliza nuestros Productos, incluso cuando se registra para crear una cuenta, crear o compartir contenido, enviar mensajes o comunicarse con otros. Esto puede incluir información presente o sobre el contenido que

> proporciona (como metadatos), como la ubicación de una foto o la fecha en que se creó un archivo. Esto también puede incluir lo que ve a través de las funciones que ofrecemos, como nuestra cámara, para que podamos tomar acciones como sugerir máscaras y filtros que le puedan gustar, o dar consejos sobre el uso de formatos de cámara. (párr. 3).

Pero eso no es todo. *Facebook* (2020a, párr. 8-10) continúa informando que también recopila datos de los dispositivos de los usuarios y que aún recibe datos personales de los usuarios de empresas colegas. La justificación, al igual que *YouTube*, va desde la provisión, personalización y mejora de los productos de la red social, hasta la investigación e innovación para el bien social.

Respecto de *Facebook* (2020a, párr. 35), informa que no vende ninguna información de los usuarios y se compromete a no hacerlo nunca, pero hace excepciones para compartir, en los siguientes casos: empresas que utilizan los servicios de *análisis* de la red social; anunciantes; empresas de medición; de bienes y servicios en productos de *Facebook*; proveedores y prestadores de servicios; investigadores y académicos; y, para la aplicación de la ley o solicitudes legales.

Cuanto a la política de exclusión de datos personales de los usuarios, *Facebook* (2020a) expone:

> [A]lmacenamos datos hasta que ya no sean necesarios para proporcionar nuestros Productos y Servicios de *Facebook*, o hasta que se elimine su cuenta, lo que ocurra primero. Esta es una determinación que varía de un caso a otro y depende de factores como la naturaleza de los datos, la razón por la que se recopilan y procesan, y las necesidades de retención operativas o legales relevantes. Por ejemplo, cuando busca algo en *Facebook*, puede acceder y eliminar esa consulta de su historial de búsqueda en cualquier momento, pero el registro de esa búsqueda se eliminará después de seis meses. (párr. 46).

En la Política de Datos de *Facebook* no se menciona el tratamiento de datos *post mortem* del usuario. Pero la Red Social no ignora la situación. En la página del “Centro de Ayuda”, *Facebook* (2020b, párr. 1) brinda al usuario la posibilidad

de indicación previa de un heredero para administrar su cuenta, que se transformará en un memorial, o solicitar la exclusión definitiva.

Facebook explica (2020b, párr. 3) que las cuentas transformadas en un memorial son un lugar donde amigos y familiares pueden reunirse para compartir recuerdos tras la muerte de una persona, pero advierte que nadie podrá ingresar a una cuenta transformada en un memorial. Esta postura, a diferencia de la presentada por *YouTube*, brinda mayor seguridad a la intimidad y privacidad *post mortem* del usuario.

El heredero previamente indicado por el usuario para administrar su cuenta de *Facebook* en caso de fallecimiento, llamado por la Red Social "contacto heredero", tendrá funciones limitadas, no teniendo acceso a la cuenta. En una página, vinculada a la Central de Ayuda, *Facebook* (2020c) determina:

> [E]l contacto heredero puede: escribir una publicación adjunta a su perfil (por ejemplo, para compartir un mensaje final en su nombre o proporcionar información sobre el funeral); actualice la foto de perfil y la foto de portada; solicitar la eliminación de la cuenta; descarga una copia de lo que compartiste en *Facebook.* (párr. 2)

Facebook (2020c, párr. 3) todavía, advierte que se pueden agregar otros recursos para los contactos herederos en el futuro, pero refuerza expresamente que el contacto heredero no podrá iniciar sesión en la cuenta, leer mensajes y eliminar amigos o hacer nuevas solicitudes de amistad. Se advierte, por tanto, que el heredero señalado por el usuario fallecido únicamente tendrá la función de gestionar el perfil transformado en memorial, sin que, no obstante, tenga acceso a datos sobre la vida privada del fallecido. Por otro lado, *Facebook*, a diferencia de *Youtube*, no acepta la posibilidad de compartir datos privados de la persona fallecida, lo que garantiza una mayor protección de la intimidad-privacidad del usuario, incluso después de su fallecimiento.

Las siguientes dos redes sociales analizadas que tienen sus políticas de privacidad y procesamiento de datos, son propiedad de *Facebook* y, por lo tanto, tienen políticas similares a la que se acaba de analizar. En cuanto a *WhatsApp* (2020a, párr. 5), la compañía explica que se incorporó a *Facebook* en el 2014, pero sigue operando en forma independiente y con un enfoque centrado en la

construcción de un servicio de mensajería que sea rápido y funcione en cualquier parte del mundo. *Instagram* (2020a, párr. 2) informa que forma parte de *Facebook* desde el 2012 y está realizando algunos cambios corporativos para que los términos reflejen que *Facebook Inc*. es responsable de *Instagram*.

WhatsApp es una aplicación de mensajería gratuita que posibilita el intercambio de audios, videos y fotos (Benitez; Cabrera; Ruidiaz, 2019, p. 11). A juicio de Lopes y Vas (2016, p. 3), *WhatsApp* en sí no es una red social, ya que su estructura es compatible con la definición de social media. Sin embargo, esta aplicación tiene la capacidad de generar innumerables redes sociales a través de la formación de grupos en su plataforma, fomentando intensamente la interacción de los participantes, es decir, los “actores sociales” involucrados.

Según el propio *WhatsApp* (2020a, párr. 1), más de dos mil millones de personas en más de 180 países utilizan *WhatsApp* para mantenerse en contacto con amigos y familiares, en cualquier momento y lugar.

En su Política de Privacidad, con versión modificada el 20 de julio de 2020, *WhatsApp* (2020b, parágrafo 3) aclara que fue compilado para no almacenar los mensajes entregados y el control que se le da al usuario para decidir quién se comunica con sus Servicios. En este sentido, *WhatsApp* (2020b) sostiene:

> [N]o guardamos sus mensajes mientras brindamos los Servicios. Una vez que se entregan sus mensajes (incluidas las conversaciones, las fotos, los videos, los mensajes de voz, los archivos y la información de ubicación compartida), se eliminan de nuestros servidores. Sus mensajes se almacenan en su propio dispositivo. Si un mensaje no se puede entregar inmediatamente (por ejemplo, si no está conectado), podemos mantenerlo en nuestros servidores hasta por 30 (treinta) días mientras intentamos entregarlo. Si el mensaje no se puede entregar dentro de los 30 (treinta) días, lo eliminaremos. (section 2, párr. 3).

Aún en los mensajes, *WhatsApp* (2020b, section 2, párr. 3) justifica que para mejorar el rendimiento y entregar mensajes con los medios de manera más efectiva, por ejemplo, al compartir fotos o videos populares, este contenido se puede almacenar en sus servidores por más tiempo que los 30 días mencionados. Aunque, por regla general, no almacena los mensajes intercambiados por los

usuarios, *WhatsApp* (2020b, section 2) asume que recibe o recopila datos cada vez que opera y presta servicios, cuando el usuario los instala, accede o utiliza. Los datos recogidos son diversos, por ejemplo, el número de teléfono y correo electrónico del usuario, lista de contactos, transacciones financieras realizadas por la aplicación, ubicación geográfica, dispositivos y redes utilizadas, *cookies* e información divulgada por terceros sobre el usuario.

Igual a las políticas de privacidad y tratamiento de datos personales ya estudiadas hasta ahora, también en su política, *WhatsApp* (2020b, section 3, párr. 1) justifica la recogida y tratamiento de los datos de los usuarios para ayudar a la empresa a operar, ejecutar, mejorar, comprender, personalizar, apoyar y publicitar sus servicios. Esta justificación es similar a la presentada para compartir los datos recopilados:

> [P]asamos a formar parte de la familia de empresas de *Facebook* en 2014. Como parte de esta familia, *Whatsapp* recibe y comparte datos con otros miembros. Podemos usar los datos que nos brindan, y ellos pueden usar los datos que compartimos para ayudarnos a operar, ejecutar, mejorar, comprender, personalizar, respaldar y publicitar nuestros Servicios y sus ofertas. (*Whatsapp*, 2020b, section 5, párr. 1).

Tampoco es posible encontrar en la política de privacidad y tratamiento de datos de *WhatsApp,* información en cuanto a la conducta de la compañía sobre los datos personales, en el caso del fallecimiento del usuario. La búsqueda en otras páginas de *WhatsApp* tampoco encuentra ninguna disposición directa sobre lo que hará con los datos del usuario fallecido. La *ausencia* de regulación por parte de la citada empresa, se justifica en la política de manejo de cuentas inactivas.

Según *WhatsApp* (2020c, párr. 1) para mantener la seguridad, limitar la retención de datos y proteger la privacidad de los usuarios, generalmente elimina las cuentas que permanecen inactivas por más de 120 días. Esto sucede cuando el usuario no se conecta a *WhatsApp* durante ese período.

Finalmente, este trabajo se centra en el estudio de la política de privacidad y el procesamiento de datos de *Instagram*. Explican Perinotto, Alves, Silva y Vieira (2020, p. 2), que, en la actualidad, la imagen fotográfica vinculada a *Instagram* se

ha convertido en una importante herramienta de difusión, llegando a infinidad de usuarios a nivel mundial. *Instagram*, es una red social que prioriza publicar imágenes y videos que los usuarios de la red ven y comparten.

A pesar de tener su propia política de privacidad y tratamiento de los datos personales de los usuarios, a la que denomina “Política de Datos de *Instagram*”, la Red Social prácticamente copia la política de la empresa propietaria, *Facebook*. Las informaciones proporcionadas al usuario por *Instagram* (2020b) sobre los datos recopilados, justificación de las recopilaciones, intercambio de datos, entre otros, son idénticas a las ya analizados anteriormente, al momento de estudiar la Política de Datos de *Facebook*.

La justificación está dada por Instragram (2020c, párr. 3) en sus "Términos de uso", donde se explica que el Servicio de *Instagram* es uno de los Productos de *Facebook*, proporcionado por *Facebook Inc*. Los Términos de Uso, por lo tanto, constituyen un acuerdo entre los usuarios y *Facebook Inc*.

Al igual que *Facebook*, *Instagram* permite al usuario fallecido mantener la Red Social en forma de Memorial:

> [L]o transformaremos en un memorial la cuenta de *Instagram* de una persona fallecida cuando recibamos una solicitud válida. Tratamos de evitar que las referencias a las cuentas convertidas en memorial aparezcan en *Instagram* de una manera que pueda molestar a los amigos o familiares de la persona fallecida. Además, tomamos medidas para garantizar la privacidad de esa persona protegiendo su cuenta. (*Instagram*, 2020d, párr. 4).

La principal diferencia entre el memorial del usuario de *Instagram* fallecido y el memorial de *Facebook*, es que *Instagram* no prevé la posibilidad de asignar un "contacto heredero" para gestionar el perfil transformado. Así, es el propio *Instagram*, el que se encarga de gestionar la cuenta del usuario fallecido, dando respuesta a las solicitudes y quejas. En este sentido:

> [L]as cuentas convertidas en un memorial son un lugar para recordar la vida de una persona fallecida. Las cuentas convertidas en memorial en *Instagram* tienen las siguientes características principales: nadie puede iniciar sesión en una cuenta convertida en memorial; la

> expresión ‘En memoria de’ se mostrará junto al nombre de la persona en el perfil; las publicaciones que compartió la persona fallecida, incluidas fotos y videos, permanecerán en *Instagram* y serán visibles para el público con el que fueron compartidas; las cuentas convertidas en memoriales no aparecen en algunos lugares de *Instagram*, como ‘Explorar’. (*Instagram*, 2020e, párr. 3).

Todas las redes sociales analizadas cuentan con políticas claras y robustas de privacidad y tratamiento de datos personales, que se presentan de forma accesible a los usuarios interesados. En todas ellas existe una recogida de datos integral que se justifica por todos, en particular, por las necesidades de mejora de los servicios y contactos con los usuarios.

El usuario menos atento no se dará cuenta de la cantidad de datos que se recopilan. Pero todos cuentan con una política que garantiza la protección de los datos personales de quienes utilizan sus servicios. Luego, en general, se cumple con las normas generales de protección de datos.

Por otro lado, cabe mencionar que las políticas de privacidad y datos de la mayoría de las redes sociales no son suficientes para convencer de que existe un tratamiento adecuado de los datos personales de los usuarios. Recientemente, varios países han comenzado a crear reglas internas más contundentes para regular estas políticas.

Argentina y Brasil son naciones que comenzaron a intervenir, por ejemplo, en las políticas de privacidad de *Facebook* y *WhatsApp*, determinando o recomendando la suspensión de la aplicación de las nuevas reglas, que entrarían en vigencia al 15/05/2021 y la sumisión de sus términos a los órganos estatales competentes. De acuerdo con la Resolución 492/2021 de la Secretaría de Comercio Interior de Argentina y la Recomendación Conjunta emitida al 07/05/2021 por la Autoridad Nacional de Protección de Datos y otros organismos estatales brasileños, la política de privacidad de *WhatsApp*, que se esperaba que estuviera vigente a partir de la fecha antes mencionada, debería suspenderse hasta nueva autorización de los respectivos gobiernos. La medida, también

implementada en otras naciones, refleja una actitud más conservadora de los Estados en un intento por proteger los datos personales de sus ciudadanos.

En cuanto a los datos personales del usuario fallecido, a partir del *análisis* de las políticas de privacidad y tratamiento de datos de las redes sociales más utilizadas en Argentina y Brasil, se concluye que las cuatro cuentan, directa o indirectamente, con políticas sobre dicha temática.

Aunque tales políticas no están dentro de las políticas de privacidad, están claramente publicadas para el usuario en otros documentos. La excepción corre a cargo de *WhatsApp*, que no tiene una política expresa sobre el tema, pero prevé la exclusión de cuentas inactivas. Entre las políticas estudiadas, se entiende que la política de *YouTube/Google* es la única que deja abierta la posibilidad de acceso de terceros a los datos de la persona fallecida.

5 Conclusión

El proyecto de protección de datos personales que presentó el Gobierno de Mauricio Macri buscaba actualizar una vieja norma del 2000, pero conservando los problemas que otras regulaciones, como la europea, procuraron corregir.

En épocas de algoritmos, convergencia y *marketing* segmentado, ya no sólo la noticia es una mercancía que se compra y se vende. Los datos personales se transformaron en un bien que se produce, se atesora, se clasifica, se comercializa y genera ganancias a las principales corporaciones del planeta.

Quien produce estos datos con las huellas de su actividad a lo largo del día, recibe a cambio, además del acceso a los servicios que son la plataforma de extracción de su información personal, publicidad comercial y política elaborada y distribuida a su medida. Los usuarios de Internet, particularmente, los de las redes sociales, son mineros digitales que, incluso cuando descansan, colaboran en el dragado del yacimiento de datos que procesa el sistema.

En este capítulo se presentó una descripción general sobre la importancia de proteger los datos personales para garantizar la intimidad y privacidad de las personas. Intensamente virtualizadas en las últimas décadas, intimidad y

privacidad han ganado contornos tecnológicos que las dejan muy ligadas a los datos personales, llegando a confundirse más de las veces, con los propios datos. Es que los datos personales son ladrillos que construyen una edificación virtual de la persona que utiliza los medios tecnológicos: la personalidad virtual.

Al igual que la personalidad real, la virtual exige protección contra el embate de quienes buscan información sobre los comportamientos del individuo. Los motivos de estos ataques son los más diversos, pero los ataques que aportan cierta importancia económica a los datos personales son los que intentan los agentes del mercado.

Se identificó que la intensa búsqueda de conductas en materia de consumo hace que los datos personales sean considerados activos importantes, con valor económico. El resultado es que se vuelven parte del patrimonio de las personas y necesitan aún más de la protección legal. Por otro lado, estaba claro que, de forma aislada, la importancia económica de los datos personales de un individuo no es robusta.

Pero esto no agota la necesidad de protección legal, ya que la característica de un bien económico es solo uno de los matices que demandan protección de datos personales. Se evidenció que, para las empresas, que son las principales responsables de la valoración económica de los datos personales, el conjunto de estos, de un individuo, solo es importante si se suma a los de otro congénere. De esta forma, las empresas pueden obtener conocimientos e informaciones importantes sobre las necesidades y requisitos de su público objetivo, optimizando sus inversiones y políticas de mercado.

Con estas poderosas, constantes y crecientes inversiones en datos personales, y con una legislación que no se mantiene al día con los avances tecnológicos, el instituto del consentimiento ha ganado protagonismo en los sistemas de protección de datos personales de Argentina y Brasil.

El ser humano se convirtió entonces en el tutor principal de sus datos personales. Pero los dos países entendieron que este rol podría ser una barrera para varios sectores y, por lo tanto, siguiendo la evolución de generaciones de leyes de datos personales, adaptaron sus legislaciones para crear alternativas

para el procesamiento de datos personales. Con ello, actualmente, el instituto de consentimiento sigue siendo la principal forma de acceso a los datos personales, pero comparte su función con varios otros institutos, que también autorizan el acceso a los datos de las personas.

Por otro lado, la evolución legislativa de Argentina y Brasil, siguiendo la tendencia internacional, dio nuevas formas a la figura del consentimiento. Actualmente el consentimiento ya no se confirma solo con acciones automáticas por parte de los usuarios de medios tecnológicos como, por ejemplo, hacer clic en una casilla de “Acepto los términos”.

En los nuevos sistemas de protección de datos personales de los dos países, el consentimiento debe obtenerse, necesariamente, a través de un acto afirmativo claro, que representa una acción inequívoca, específica, libre e informada, bajo pena de ser considerado nulo. Por este motivo, las empresas e instituciones que se ocupan de los datos personales vienen promoviendo ajustes intensos de sus políticas de datos a la nueva realidad de los sistemas de protección de datos en Argentina y Brasil.

No es diferente con las redes sociales. También han estado promoviendo adaptaciones considerables en ambos países. En el contexto de una intensa búsqueda de datos personales agregados, son los principales agregadores, ya que recopilan y reciben grandes volúmenes de datos personales, de los más diversos órdenes, de los usuarios.

Con esto, las redes sociales son capaces de generar un perfil virtual casi completo de sus usuarios, lo que exige políticas robustas de privacidad y tratamiento de datos de los usuarios, con el fin de tener una adecuada protección y cumplimiento de las leyes de protección de datos.

Del análisis realizado en las redes sociales más utilizadas en Argentina y Brasil (*YouTube*, *Facebook*, *Whatsapp* e *Instagram*), se concluye que todas cuentan con políticas de privacidad y tratamiento de datos personales robustas y similares. Se encontró aún, una recopilación de datos enorme y más allá de la impresión común de que solo se recopilan datos relacionados con el servicio al que accede el usuario.

Por esa misma razón, dichas políticas de datos deben ser, y son, verdaderamente sólidas, claras y bastante accesibles para los usuarios que deseen conocerlas. Estas políticas contienen información sobre todos los datos que se recopilan, los motivos de la recopilación, las posibilidades de compartir los datos, la gestión compartida con los titulares de los datos, la posibilidad de exclusión, entre otros.

Sobre al tratamiento de los datos personales del usuario después de su muerte, tema de mayor interés para el objeto central de este trabajo, se notó que las redes sociales que tuvieron sus políticas de privacidad y tratamiento de datos analizadas, tienen comportamientos diferentes. *YouTube*, la red social más utilizada en Argentina y Brasil, no tiene una política clara sobre el tratamiento de los datos del usuario fallecido, dejando a su discreción analizar las solicitudes que se le presenten.

Facebook e *Instagram* tienen políticas similares, que permiten la eliminación o transformación del perfil del usuario fallecido en un memorial. La principal diferencia entre las políticas de las dos redes sociales está en la administración del memorial del usuario fallecido, ya que, mientras *Facebook* prevé la figura de un “contacto heredero” para gestionar el memorial de forma limitada, *Instagram* deja bajo su responsabilidad la administración del perfil.

Por último, *WhatsApp* no tiene ninguna política directa de tratamiento de datos de usuarios *post mortem*, pero sí se compromete a eliminar las cuentas inactivas después de 120 días sin acceso, lo que termina reflejándose indirectamente en las cuentas de los usuarios fallecidos.

Capítulo IV: La utilidad de los datos de personas fallecidas alojados en Internet

1 Introducción

En este capítulo, se abordará el problema central de la tesis con respuestas sobre la protección de la intimidad y privacidad a través de los sistemas jurídicos de protección de datos existentes en Argentina y Brasil; si bien, previamente, se hará una presentación señalando la importancia de los datos de las personas fallecidas. Se explorarán ejemplos como los mencionados para demostrar que existe un uso creciente de este tipo de datos, y que este uso requiere una protección legal efectiva, bajo pena de violación de la intimidad-privacidad del fallecido.

El enfoque de los sistemas jurídicos argentino y brasileño para la protección de datos personales tendrá como objetivo presentar hasta qué punto los dos países están preparados para proteger la intimidad y privacidad *post mortem* en la actualidad. Se estudiarán las leyes de protección de datos personales existentes, y los proyectos de ley que abordan la materia, con el objeto de trazar un panorama actual y futuro, de cómo se han preocupado las naciones en resolver la temática en cuestión.

Finalmente, considerando la hipótesis de que Argentina y Brasil aún no cuentan con la protección legal adecuada para la intimidad-privacidad de las personas fallecidas, se llevará a cabo una investigación sobre el instituto del “Derecho al Olvido”, como una forma alternativa de proteger los datos personales después de la muerte.

Aún de aplicación divergente, el “Derecho al Olvido” garantiza a las personas vivas el ocultamiento de situaciones que no desean compartir más. En el caso de personas fallecidas, la aplicación de este derecho puede ser una medida eficaz para resguardar la información, lo cual ya lo hacen, por ejemplo, algunas redes sociales, como lo explicara en el capítulo anterior.

2 ¿Para qué sirven los datos de las personas fallecidas guardados en Internet?

La vida moderna trastocó aquellos conceptos históricamente consolidados, impregnándolos de incertidumbre, producto del impacto de las nuevas tecnologías en la vida cotidiana. De esta forma, la ruptura de los grandes paradigmas sociales produjo significativos cambios, con consecuencias materiales y existenciales para toda la humanidad.

Las relaciones de trabajo, consumo, salud, afectivas, empresariales y estatales son ejemplos de situaciones que han sido modificadas profundamente por la revolución tecnológica. A ello se suman los problemas relacionados con el individuo, como la privacidad y la intimidad, los que también sufren la disrupción causada por la tecnología, al transitar por espacios hasta hoy desconocidos.

Bertoni y Cortés Castillo (2014) critican el hecho de que la actividad humana está cada vez más documentada en la red, largas porciones de ésta quedan fuera de ese registro: conversaciones personales, encuentros, movimientos, actividades cotidianas y, sobre todo, las interpretaciones y sensaciones del individuo. Pero a medida que pasa el tiempo la memoria digital nos ofrece siempre el mismo recuerdo: el mismo video o el mismo intercambio de mensajes. Nuestra memoria se condiciona entonces a los episodios registrados y deja de lado los demás. Tomamos como referente del pasado un recuerdo objetivizado en detrimento del subjetivo y personal (p. 133).

Según Bertoni y Cortés Castillo (2014, pp. 133-134) ese pasado estático –argumentan algunos autores– se vuelve un obstáculo para el desarrollo personal. Teniendo un referente tan aparentemente claro de lo que hizo o pensó en el pasado, el individuo no se permite olvidar o cambiar.

Igualmente merecen ser consideradas cuestiones aún más profundas, ya que la tecnología ha estado creando situaciones antes inimaginables. Este es el caso de la propia existencia humana. Partiendo de la lógica y alejándose de cualquier convicción religiosa, la estancia de una persona en el plano terrestre dura hasta su muerte. Es decir, por sentido común, termina con la muerte; en

síntesis, y sin otra consideración, es el fin de la vida terrenal. Durante siglos, esto ha sido prácticamente incuestionable.

A pesar de la muerte, el cuerpo, la imagen y la memoria de la persona pueden influir en el rumbo social y perdurar en el mundo de las relaciones jurídicas, más allá que el titular ya no sea sujeto de derechos, y merecedor de una protección jurídica autónoma (Beltrão, 2015, p. 2).

Para Cobiella (2013, p. 114) cada cultura tiene su propia forma de entender la muerte y la vida. El Derecho no ha permanecido inmune a sus efectos, teniendo en cuenta el acompañamiento que éste hace a las personas, antes de nacer, durante su vida, y por supuesto luego de la muerte, con la apertura de la sucesión. Por ello, Zampier (2021, p. 121) hace la reflexión de que, en la sociedad de la información, la muerte comienza a verse de una manera nueva, al menos si se la compara con la tradición de los últimos siglos en la parte izquierda del planisferio.

La revolución tecnológica trae un gran desafío a esta verdad. La enorme recopilación de datos personales, que crea perfiles y personalidades virtuales, asociados a tecnologías como la inteligencia artificial y la robótica, prolongan, aunque artificialmente, la presencia física y digital de las personas, incluso después de su muerte.

Los robots humanoides equipados con inteligencia artificial, capaces de utilizar datos recopilados, ya están en el mercado para ser adquiridos con la apariencia que ordena el cliente. Se puede acceder a las propiedades intelectuales almacenadas en forma de datos, creando obras artísticas de autores muertos. Las imágenes de artistas ya fallecidos se explotan comercialmente a través de la proyección mediante hologramas y otros medios tecnológicos.

Estos son solo algunos ejemplos del uso de la tecnología para mantener la presencia, entre los vivos, de personas ya fallecidas. Las situaciones narradas traen, por sí mismas, una gran preocupación por la vulneración de la intimidad y privacidad de quienes ya no pueden oponerse al acceso a sus datos.

La preocupación también existe, asimismo, cuando no hay un propósito económico para acceder a información privada. La divulgación de secretos puede generar disgustos que ciertamente no serían causados por el titular de la

información. De ahí la necesidad de analizar el alcance de la protección legal existente, respecto de la intimidad-privacidad.

Destaca Cobiella (2013, p. 115) que, dejando clara la cuestión de que con la muerte se extingue la personalidad, aparece la problemática jurídica, de extender esta protección más allá del fallecimiento de quien fuera titular de determinados derechos (honor, intimidad, privacidad e imagen); los llamados derechos de la personalidad.

Silva y Doto (2017, p. 1) sostienen que, ante la constante y rápida evolución tecnológica, la ley y la protección jurisdiccional del Estado no garantizan la protección e inviolabilidad de la intimidad, la privacidad, el honor y la imagen de la persona. A ello se suma la lentitud burocrática legislativa en la aprobación de nuevas leyes, surgiendo la anomia normativa, producto de la ausencia de nuevas reglas que tengan por objeto, la satisfacción de la protección del individuo.

La experiencia de la lentitud narrada se vive en Argentina y Brasil, ya que los dos países han tardado en avanzar y adecuar sus respectivos ordenamientos jurídicos a las diversas problemáticas sociales que trae la tecnología. El problema que guía este trabajo es solo un ejemplo del retraso y la falta de estándares relacionados con los avances tecnológicos en ambos países. Si cuestiones urgentes y menos complejas, como la protección de los datos de las propias personas vivas, aún esperan una protección estatal satisfactoria, es posible que los asuntos relacionados con las personas fallecidas no se regulen adecuadamente en poco tiempo.

De acuerdo con Cobiella (2013, p. 114) la muerte produce determinados efectos relacionados, la mayoría, con el patrimonio, y otros (menos conocidos, pero por ello no menos importantes), con la propia esencia del ser humano; los llamados derechos de la personalidad. Ello desencadena un conjunto de efectos, que, a simple vista, parecen sencillos, pero que en la práctica jurídica llaman la atención; cuestión que no ha sido ignorada ni por la doctrina, ni por la jurisprudencia.

Estos efectos se relacionan con la aparición, transmisión o extinción de distintos derechos. Por una parte, se encuentran derechos que permanecen y se

transmiten; otros derechos se extinguen con la muerte, mientras que otros se adquieren con ocasión de la muerte de una persona, pero no en virtud de sucesión mortis causa, como las pensiones de viudez u orfandad; el seguro de vida para caso de muerte del asegurado. Los derechos de la personalidad no se mantienen al margen de esta cuestión. La razón se encuentra en todo aquello perdurable, aun después de muertos (Cobiella, 2013, p. 114).

En esta línea, Zampier (2021, p. 126) advierte que están en juego diversos intereses de los familiares, del propio fallecido, terceros, y de los proveedores de servicios de Internet.

Cabe mencionar que la protección *post mortem* de ciertos bienes de la personalidad concierne a los intereses propios de la persona, mientras está en vida, como una valoración de los elementos que la individualizaron como ser humano, sujeto a un trato digno antes y después de su muerte. En efecto, el cuerpo muerto y su memoria necesitan el mismo respeto a la dignidad que fue sometido a la persona viva, en la cara de su cuerpo y su honor (Beltrão, 2015, p. 2). Al mismo nivel, también existe la necesidad de proteger la intimidad y privacidad, que, como otros derechos de la personalidad, exigen la continuación de la protección legal después de la muerte.

Al mismo tiempo, se debe tener en cuenta que las tecnologías de la información pueden crear una vulnerabilidad en el espacio privado, en lugar de expandirlo, ya que los hábitos de consumo de los individuos pueden ser investigados por las empresas, las que, a través de herramientas virtuales, monitorean tales hábitos, impulsando a las personas a contratar cada vez más. La riqueza de la esfera privada en la sociedad de la información es frágil y está expuesta a peligros. Esto justifica la necesidad de fortalecer la protección legal, así como de extender la frontera de la ley de privacidad (Zampier, 2021, p.138).

La tecnología e Internet están a menudo a años luz de las normas que regulan la conducta social, que tienen pocas leyes prácticas y pocas limitaciones sobre la conducta ilegal. La falta de normas regulatorias incentiva y permite el acceso y uso de la imagen ajena, principalmente en redes sociales y medios digitales (Silva; Doto, 2017, p. 1).

A partir de estas reflexiones es posible identificar qué parte de la doctrina ha acercado algunos derechos de la personalidad, como la privacidad, al concepto de bien digital. Cabe recordar que la protección de este instituto no se da únicamente en la esfera virtual, ya que aún puede existir una violación por el acceso indebido a la correspondencia, diarios y otros documentos físicos y confidenciales. Pero el tratamiento de la privacidad y de los datos personales como activos digitales es, de hecho, algo que ha ido ganando fuerza con la revolución tecnológica.

En este sentido, Zampier (2021, pp. 116-117) explica que cuando la información insertada en la red mundial sea capaz de generar repercusiones no patrimoniales, se debe entender que será un activo tecno-digital existencial.

Continúa Zampier (2021):

> [T]odo ser humano, desde el momento en que se convierte en usuario de Internet, tendrá la posibilidad de titularizar activos digitales de carácter muy personal. Y este movimiento es muy común en la actualidad, con la proliferación [...] de redes sociales. El sujeto subirá fotos, videos, expresará sus emociones, pensamientos, ideas, intimidad, con un número ilimitado de personas. Este conjunto de atributos no patrimoniales, digitalizados a lo largo del tiempo, formaría la noción de bien tecno-digital existencial. (p. 117)

En la misma idea de acercarse la privacidad del concepto de bienes digitales, Font y Boff (2019, p. 33) sostienen que son de naturaleza personal los bienes no patrimoniales que pueden estar protegidos dentro de cuentas de redes sociales, como fotografías e información digital, copias de seguridad de herramientas de comunicación, claves de firma electrónica, entre otras. También podrán estar contenidos otros tipos de informaciones que tienen una naturaleza jurídica difusa, dado su carácter personal y su valor patrimonial, como la información confidencial sobre un determinado proceso industrial, los resultados de una investigación periodística o novela y documentos encriptados con valor económico, entre otros. Estos últimos también se denominan bienes digitales de contenido mixto, entre los que se puede mencionar los derechos de autor, específicamente los derechos patrimoniales, así como la legitimación reconocida para la defensa y protección de la obra (integridad y paternidad) posterior al fallecimiento del autor.

Según Font y Boff (2019, p. 56), existen una multiplicidad de bienes digitales, con diversas características; clasificados en personales, no personales y de naturaleza mixta. Solo aquellos que son susceptibles de valoración económica podrán ser transmitidos en la herencia digital, creándose dudas en relación con la defensa y protección de aquellos que no tienen este carácter. Las normas de defensa de la memoria pretérita y de protección de datos personales no son suficientes para garantizarla.

Resulta imposible en este ámbito desconocer la relación que tiene lugar entre los bienes digitales personales y el acceso a cuentas y servicios susceptibles de valoración económica, así como el respeto de la privacidad y de las comunicaciones del titular de dichas cuentas una vez fallecido (Font; Boff, 2019, p. 34).

Por lo expuesto, se concluye, que la privacidad también será considerada un activo digital, sin valor económico estimado, pero con repercusiones en el ámbito jurídico del individuo. Por ello, debido a la ausencia, en teoría, de valor económico, la privacidad no estaría enmarcada en el concepto de herencia digital; no siendo posible su inclusión, en el orden sucesorio.

En cambio, no sucede lo mismo con los datos personales –como ha sido señalado en el capítulo anterior–, ya que pueden tener cierto valor económico y, de acuerdo con las ideas aquí presentadas, podrían integrar el patrimonio digital del individuo para ser heredado por sus sucesores cuando él fallezca. El gran problema es que los datos personales a menudo conllevan el potencial de violación de la intimidad y privacidad, ya que también agregan información que es de naturaleza íntima, cuya divulgación podría no ser de interés para el titular ahora fallecido.

El avance de la inserción de las tecnologías digitales en la vida de las personas genera una intensa virtualización de las acciones íntimas y las relaciones sociales de los individuos, provocando que surjan situaciones diversas, al menos curiosas, relacionadas con la intimidad-privacidad y los datos personales, que necesitan de tutela estatal con urgencia. Varios ejemplos de estas situaciones se presentan en películas futuristas, generalmente de ciencia ficción.

Resulta que ellos ya no se insertan adecuadamente en la idea de futuro y ficción, y ya ocurren hoy.

En la futurista serie inglesa *Black Mirror*, las ideas relacionadas con los problemas provocados por los avances tecnológicos generan profundas reflexiones de las más diversas órdenes.

Explica Silva (2020, p. 10) que esta serie, ahora disponible en varios países en la plataforma de *streaming Netflix*, subvenciona, a través de sus tramas, la concepción de que Occidente se ha rendido a las sentencias de una crisis ética, marcada principalmente por una rarefacción de las convenciones sociales, por una resignación al individualismo y decadencia de la alteridad. La contigüidad de los mecanismos que componen el "mundo digital", ambientado en los guiones de Black Mirror, ha surgido, incluso entre sus fanáticos, la jerga "esto es muy *Black Mirror*", utilizada cuando algún evento de la "vida real" alude al tema central de la serie.

En el episodio titulado *"Be Right Back"* (*Netflix*, 2013), una joven (Marta) ve en la inteligencia artificial la oportunidad de volver a ver a su esposo (Ash), que murió temprano en un accidente automovilístico. Igualmente, la posibilidad, que inicialmente encanta a la protagonista y espectadores de la segunda temporada resulta amarga, a medida que ella se involucra con el "clon" de su pareja (Veja, 2017, 8º párr.).

La siguiente narrativa ilustra lo que sucede en el episodio:

> [E]l software procesa Ash digital de todo lo que él había publicado en las redes sociales y registrado en correos electrónicos. De sus pistas digitales, de la información que sobrevive a la vida de su cuerpo, Ash resucita. El programa también comenta con Marta sobre la extrañeza del aspecto fantasmal y espectral de estos contactos telefónicos con la voz de un muerto. La credibilidad del Ash digital está garantizada no solo por su voz, sino también por la emulación del humor dulce y cáustico, muchas veces dirigido a sí mismo, que caracterizaba al chico. Por ejemplo: en la primera llamada, la voz le dice a Marta que debe ser extraño que él pueda hablar, ya que ya no tiene boca, un tipo de humor compatible con lo que Ash podría decir en una situación como esa. En otras palabras: el software no

> solo imita lo que el personaje ha escrito; emula creativamente tu estilo. Cuando Marta hace una ecografía, escucha el corazón del feto y graba el sonido para enviárselo a Ash. Sin embargo, el celular cae al suelo, se pierde el contacto y ella se da cuenta de la fragilidad de este modo de sustitución. Este es el momento oportuno para que el software te venda (y bastante cara) una solución tecnológica aún más perfecta y tangible: un cuerpo biosintético idéntico al de tu compañero muerto, capaz de soportar el programa con más estabilidad, efectividad y probabilidad. Marta acaba adquiriéndolo. (Ferraz, 2019, pp. 64-65).

La dinámica del episodio analizado, aunque parece alejada de la realidad, es algo que ya ocurre. Rocha (2017, párr. 1) informó que una aplicación surcoreana te permite hablar e incluso tomar una selfie con alguien que ha fallecido. La noticia publicada en el sitio *web* brasileño Olhar Digital muestra que la aplicación *With Me* escanea en 3D y recrea digitalmente a las personas mientras aún están vivas. Luego, el avatar está disponible digitalmente, pudiendo responder a gestos, palabras e incluso posar para una foto con el usuario.

Calais (2020, párr. 4) informó en la columna Insider, de la revista Forbes, que Deibson Silva, un investigador y neuropsicólogo brasileño, fundó una startup para recrear personas muertas. La *startup Legathum*, desarrollada en Silicon Valley, tiene como objetivo mapear la personalidad humana y transferir todo eso a la inteligencia artificial.

Es un hecho que las tecnologías mencionadas tienen la inteligencia artificial como herramienta principal, lo que deja los servicios ofrecidos limitados al mundo virtual. El problema es que los avances tecnológicos no se detienen ahí. La inteligencia artificial asociada con la robótica y otras tecnologías puede transformar la existencia virtual en presencia física.

Ghosh (2020, párr. 7) informó en el sitio *web* de *BBC News* que *Realrobotix*, una empresa con sede en Estados Unidos, publicó un video promocional del robot *Harmony* (robot sexual de aspecto humano con inteligencia artificial), a la venta a precios que van desde los 8.000 hasta 10.000 dólares. La noticia también dice que *Harmony* es una muñeca de tamaño natural que puede parpadear y mover los ojos y el cuello, así como los labios mientras habla.

La realidad virtual también es una tecnología que, asociada a otras, puede brindar experiencias similares a las retratadas en el episodio de *Black Mirror*. *BBC News* (2020) informó el 19 de febrero de 2020: "La madre 'encuentra' a su hija muerta con la ayuda de la realidad virtual en un programa de televisión".

Según la noticia, Jang Ji-sung quería una última oportunidad para despedirse de su hija de 7 años, Na-yeon, quien murió repentinamente en 2016, de un trastorno sanguíneo incurable. El documental, llamado *"Meeting You"*, se estrenó en la televisión surcoreana MBC y grabó el encuentro de Jang Ji-sung y Na-yeon. También según la BBC (2020), la tecnología de captura de movimiento se utilizó para grabar los gestos de una actriz infantil, que luego se utilizaron para recrear los movimientos de Na-yeon. También se reprodujo la voz de Na-yeon.

Se observa que la tecnología existente ya es capaz de mantener la presencia artificial de una persona después de la muerte, aunque todavía existen limitaciones. Pero el rápido avance tecnológico sugiere que, a partir de ahora, la mencionada presencia tendrá mejoras que la harán cada vez más real y accesible.

Resulta que, en todos los ejemplos citados, los medios tecnológicos no funcionarían si no fueran alimentados por los datos de la persona fallecida. La imagen, la voz, la ubicación, las consultas, las conversaciones y todo lo demás disponible o almacenado en Internet y los dispositivos informáticos son cruciales para que los productos y servicios tecnológicos logren su propósito. Es decir, sin los datos personales del fallecido, su presencia artificial no existiría. Es este el punto en el cual la protección de datos se comunica con la protección de la intimidad y la privacidad *post mortem*.

Pero eso no es todo. El acceso a los datos de la persona fallecida, en otras ocasiones puede ocasionar serias limitaciones y violaciones de la intimidad-privacidad. Zampier (2021, pp. 126-128) da tres ejemplos de situaciones relacionadas con la muerte y los activos digitales, que también involucran problemas de intimidad y privacidad para las personas fallecidas.

En el primer ejemplo, un militar muere en una guerra y sus sucesores (esposa y padre) obtienen una orden judicial para acceder a su cuenta de correo electrónico. Al acceder a los datos proporcionados por el proveedor de servicios

de Internet, descubren que el soldado muerto tenía una aventura homosexual con un colega de las Fuerzas Armadas y que buscaba una manera de desertar y abandonar la misión, provocando infelicidad en su esposa y disgusto en su padre.

El segundo ejemplo involucra a una escritora famosa que, en su vida, siempre había dejado claro que no quería que se publicara ninguna obra inacabada. Después de su muerte, su único hijo obtuvo, del proveedor del servicio de almacenamiento digital, “nube”, autorización para acceder a los contenidos allí almacenados por la madre fallecida. En ese momento, encontró una obra inacabada y la vendió por una cantidad considerable a una editorial internacional.

En el último ejemplo, una joven muere en una fiesta por consumo de alcohol, y sobredosis de drogas. Los padres, al enterarse de algunos comentarios hechos en el perfil de *Facebook* de su hija, luego de su muerte, solicitaron el borrado de la cuenta y el acceso a los datos en un intento por comprender lo sucedido. Al acceder a los datos, su sufrimiento aumentó al ver fotos de la hija caída en la fatídica fiesta, probablemente ya muerta.

Las situaciones aquí descritas muestran la profundidad del problema creado en la sociedad de la información que involucra la protección de datos personales y la intimidad-privacidad *post mortem*. Los datos tienen el potencial de sumar valores económicos y patrimoniales y, por tanto, son objeto de varios intereses, como los del mercado.

Por otro lado, también cuentan con información que, aunque no de la misma importancia, encierra secretos y el historial de la persona fallecida, que puede ser objeto de acceso indebido y vulneración de los derechos de la personalidad. No en vano empiezan a surgir negocios orientados a procesar datos sobre personas fallecidas, lo que demuestra que estos activos no pueden descuidarse.

Algunos prestadores de servicios han establecido su modelo de negocios a partir de brindar servicios como gestores de cuentas digitales *post mortem*, incluso suelen hablar de testamentos digitales. La desprotección que existe en relación con este particular en los ordenamientos jurídicos latinoamericanos puede provocar la proliferación de estos negocios digitales, con la consecuente

desprotección de las personas que confían en estos servicios (Font; Boff, 2019, p. 36).

Resulta claro que no existen instrumentos jurídicos que permitan de manera efectiva garantizar el cumplimiento y la efectividad de las disposiciones realizadas al amparo de los contratos de prestación de servicios suscritos con estas empresas. La situación puede ser más complicada cuando estas se extinguen o liquidan. Habría que acudir al cumplimiento de los contratos firmados para garantizar debidamente la voluntad digital *post mortem*. Pero todo ello solo es posible si existiera un conocimiento sobre estos por parte de los herederos, quienes subrogándose en lugar y grado del titular de las cuentas y servicios pudieran conminar al cumplimiento del contrato en su día firmado por aquel con la respectiva empresa (Font; Boff, 2019, p. 36).

El alcance de la importancia de los datos de una persona fallecida va más allá de lo que se presenta aquí, y otras acciones pueden basarse en el acceso a este tipo de información. Este es también el caso de ejemplos de investigaciones penales, acceso al historial de salud familiar y conocimiento sobre los comportamientos de los consumidores. Existen innumerables posibilidades de utilizar información relacionada con el fallecido.

Se demuestra entonces que es de gran relevancia la necesidad de una normativa legal capaz de garantizar la continuidad de la circulación de los datos a partir de sucesores y, al mismo tiempo, preservar la intimidad y privacidad del extinto. La materia es de profunda complejidad, pues exige una delicada compatibilidad entre los derechos patrimoniales y de la personalidad, en un contexto social que no tiene paradigmas, principalmente porque ocurre en un momento en que el mundo atraviesa una revolución tecnológica.

3 El tratamiento jurídico dado por Argentina y Brasil respecto de los datos e informaciones privadas de las personas fallecidas guardadas en Internet

El Código Civil brasileño, en su artículo 6, declara que la existencia de la persona natural termina con la muerte y, en consecuencia, termina su personalidad civil, provocando que la persona deje de ser sujeto de derechos y

obligaciones. La calidad de sujeto de derechos es fundamental para que la persona pueda proteger sus bienes e intereses legales (Beltrão, 2015, p. 2).

Por lo tanto, es necesario comprobar que, hoy en día, existe para muchos una vida en el mundo virtual tan o más activa que en el mundo concreto, por así decirlo, que no deja de existir, sincrónicamente, con la muerte del cuerpo físico, al menos de alguna manera (Beppu; Maciel, 2020, p. 6).

En el mismo sentido, al comentar sobre el artículo 93 del Código Civil y Comercial argentino, que también establece que la existencia de la persona humana termina por su muerte, Herrera (2015), dice:

> [A]sí como a la legislación civil le interesa el comienzo de la persona humana, también le interesa lo relativo a su extinción, ya que el fin de la existencia de la persona trae consigo el cese de la personalidad e importantes consecuencias jurídicas en el campo del derecho en general; y en el civil, de manera particular. Por citar una modificación sustancial, pasa a regir un plexo normativo propio como lo son las disposiciones referidas al derecho sucesorio que se encuentran concentradas en el Libro V, Transmisión de derechos por causa de muerte. El fin de la existencia de la persona humana se relaciona con un hecho biológico: la muerte o fallecimiento. (p. 191).

Ambos países tienen tratamientos similares, respecto al fin de la existencia humana, incluyendo otros institutos vinculados a ella, a saber, la ausencia y la muerte presunta. También regulan de manera aproximada la protección de los derechos de la personalidad después de la muerte.

Diniz (2017, p. 9) recuerda que los derechos de la personalidad son derechos comunes de la existencia, porque son simples permisos dados por la norma jurídica, a cada persona de defender un bien que la naturaleza le dio, de manera directa y primordial.

En el caso de las personas fallecidas, el Código Civil brasileño, en el artículo 12, garantiza a los herederos la defensa de los derechos de la personalidad, disponiendo que se puede exigir que cese la amenaza, o la lesión, al derecho de la personalidad, y reclamar pérdidas y daños sin perjuicio de otras sanciones previstas por la ley.

En la misma línea, el Código Civil y Comercial argentino tutela expresamente la defensa del derecho a la imagen por los herederos o causantes, en el artículo 53, estableciendo que en caso de personas fallecidas pueden prestar el consentimiento sus herederos o el designado por el causante en una disposición de última voluntad.

En este contexto, se considera que, en caso de las personas fallecidas, en Argentina y Brasil, la violación de su intimidad-privacidad por medio de las redes sociales o cualquier otro mecanismo de Internet, legitima a sus sucesores a reclamar la reparación o cese del daño o amenaza, ya que se trata de lesionados indirectos.

El lesionado indirecto es aquella persona que padece un daño propio, derivado de un ilícito que tiene por víctima a una tercera persona, en relación a la cual hay un vínculo de naturaleza patrimonial o no patrimonial que resulta afectado. Este es el llamado daño reflejo, pues el daño proviene de una situación jurídica objetiva que vincula al lesionado indirecto y la víctima directa. También conocido como daño por rebote, considerando que la lesión alcanza inmediatamente al individuo A, pero indirectamente alcanza intereses dignos de protección de B, que de alguna forma está ligado (Farias, Rosenvald, y Neto, 2016, p. 332).

Así, las personas legitimadas tienen como función principal la defensa de la memoria una vez que se ha corroborado la existencia de una vulneración de las expresiones *post mortem* de lo que un día fueron los derechos de la personalidad de una persona determinada (Font; Boff, 2019, p. 35).

No hay grandes dificultades para entender que, después de la muerte, los derechos de la personalidad, incluidas la intimidad y privacidad, tienen protección legal, que deben reclamar los sucesores de la persona fallecida. Sin embargo, debido a su generalidad, dicha protección se vuelve insatisfactoria cuando se aplica a la protección de los datos personales *post mortem*. Es necesario un gran esfuerzo para vincular los datos personales con los derechos de la personalidad y, con ello, encontrar un uso práctico de las disposiciones legales aquí mencionadas.

En cuanto a las reglas del derecho sucesorio, para Font y Boff (2019, p. 35), la aplicación rígida no tiene cabida hoy en el ámbito digital, en particular en la relación que tiene lugar entre la protección de la identidad digital *post mortem*, la transmisión *mortis causa* de los bienes digitales susceptibles de valoración económica, el respeto de la intimidad-privacidad del titular fallecido y el correspondiente poder de disposición que este tuvo sobre dichos bienes.

Por muy técnica que sea la interpretación de las normas que protegen los derechos de la personalidad, no habrá una protección adecuada de los datos personales con el uso de estas leyes genéricas. Por lo tanto, es necesario buscar en las leyes de protección de datos específicas de Argentina y Brasil una normatividad más específica y efectiva, especialmente en lo relacionado con los datos personales de un titular extinto.

Así también, la protección de los datos de carácter personal es resistida por sectores interesados en almacenar datos personales y usarlos de diferentes formas: para controles abusivos de los gobiernos y aparatos estatales que acumulan información con la intención de manipular a los titulares de esos datos, con la egoísta intención de conservar su poder, para proteger intereses comerciales del mundo empresarial u otras causas que, bajo la aparente vocación por el progreso y la investigación científica, violan derechos humanos esenciales (Saltor, 2013, pp. 34-35).

En el contexto del ordenamiento jurídico argentino, la Ley 25.326 “de Protección de los Datos Personales”, en el artículo 14, garantiza a los sucesores universales el derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes. Es el llamado derecho de acceso, cuya respectiva disposición legal establece lo siguiente:

> [A]rtículo 14. — (Derecho de acceso).
> 1. El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes.

> 2. El responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente.
> Vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará expedita la acción de protección de los datos personales o de hábeas data prevista en esta ley.
> 3. El derecho de acceso a que se refiere este artículo sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto.
> 4. El ejercicio del derecho al cual se refiere este artículo en el caso de datos de personas fallecidas le corresponderá a sus sucesores universales.

Cabe recordar aquí que la negativa al cumplimiento de este derecho es una posibilidad prevista en el derecho argentino, que fue objeto de estudio en el punto 2 del capítulo II de esta tesis. Advierten Font y Boff, (2019, p. 46) que, en Argentina, a partir de lo previsto en el artículo 14.4 de la Ley 25.326 (Ley de Protección de los Datos Personales), los sucesores universales pueden ejercer el derecho de acceso a los datos de las personas fallecidas; aunque la norma no establece el alcance de este acceso, ni cómo se realizará el mismo.

Tanús (2002, párr. 105) deja claro que, de acuerdo a lo establecido por el artículo 14 del Decreto 1558/2001, siempre que se garantice la identificación del titular o, en caso de personas fallecidas, el vínculo correspondiente con la presentación de la declaratoria de herederos, la solicitud de información no requiere de fórmulas específicas y puede efectuarse de manera directa, presentándose el interesado ante el responsable o usuario del archivo, registro, base o banco de datos, o de manera indirecta, a través de una intimación fehaciente por medio escrito que deje constancia de su recepción.

Según Tanús (2002):

> [E]l acceso podrá consistir en la mera consulta de los archivos por medio de la visualización, o en la indicación de los datos objeto de tratamiento por escrito, por medios electrónicos, telefónicos, de imagen u otro idóneo a tal fin y, de acuerdo a lo establecido por el Decreto reglamentario, permitirá que el titular de los datos:

> 1) Conozca si se encuentra o no en el archivo, registro, base o banco de datos.
> 2) Conozca todos los datos relativos a su persona que consten en el archivo.
> 3) Solicite información sobre las fuentes y los medios a través de los cuales se obtuvieron sus datos.
> 4) Solicite las finalidades para las que sus datos fueron recabados.
> 5) Conozca el destino previsto para sus datos.
> 6) Sepa si el archivo se encuentra registrado en el registro habilitado por la Dirección Nacional de Protección de Datos Personales. (párr. 106).

Asimismo, la normativa argentina aún no es clara en cuanto a la extensión del derecho de acceso en el caso de los datos de una persona fallecida, lo que termina dificultando a los sucesores el ejercicio de este derecho. En el proyecto de la nueva Ley de Datos Personales de Argentina (2018) tampoco se supera la oscuridad de la norma, ya que el texto del artículo 27 limita el requerimiento del titular de los datos -previa acreditación de su identidad-, a solicitar y obtener el acceso a sus datos personales que sean objeto de tratamiento.

La incompletitud normativa termina prolongando los conflictos relacionados con el acceso a los datos personales del fallecido. En la opinión de Font y Boff (2019, p. 31), la relación que existe entre los proveedores de servicios y el titular de los bienes, incluyendo cuentas y datos resulta intransmisible por su carácter contractual. Los primeros esgrimen que estos contratos tienen el carácter de personalísimos sin indicar el fundamento de esta decisión más allá de lo dispuesto en los términos y condiciones, donde además nada se dice sobre el destino de estos bienes posterior al fallecimiento de su titular. [...] Cuando los herederos intentan acceder a estos datos, dichos proveedores argumentan que en virtud del derecho a la intimidad y privacidad del titular fallecido no es posible conceder el acceso, aun cuando no queda tampoco claro si estos continúan o no tratando los datos personales asociados a estas cuentas y servicios.

Complementa Zampier (2021, p. 256), argumentando que los proveedores de Internet tendrían interés en no otorgar acceso a terceros, ajenos al titular de la cuenta, sea por respeto al contrato de adhesión estipulado, sea por los gastos

económicos que implica la operatividad de miles de pedidos que llegarán rutinariamente a sus oficinas.

El artículo 34 de la nueva versión del anteproyecto de Ley de Protección de los Datos Personales, resultado de la consulta pública de febrero de 2017, contempla la posibilidad de que el ejercicio de los derechos de acceso, de rectificación, oposición, supresión, valoraciones personales automatizadas y portabilidad de datos personales puedan ser ejercidos por los sucesores universales del titular de los datos.

Según el artículo 20.2 del citado anteproyecto (posteriormente modificado al artículo 81), estas mismas personas están legitimadas para ejercer la acción de habeas data por el titular de los datos afectados. Entre los legitimados para el ejercicio de los derechos se encuentran los causahabientes siempre y cuando acrediten tal condición (Font; Boff, 2019, pp. 46-47).

Sin claras especificaciones, la ley argentina protege superficialmente el tratamiento de los datos del fallecido. Las reglas existentes no son claras y generan conflictos como el descrito anteriormente. Por más que la Ley de Protección de los Datos Personales del país prevé el derecho de los sucesores a acceder a los datos personales del fallecido, y el proyecto de la nueva ley amplía la lista de derechos que pueden ejercer los herederos, el asunto sigue estando insuficientemente protegido.

Principalmente en lo que respecta al derecho de acceso, no existe una armonización con los derechos de la personalidad, ya que el pleno cumplimiento de ese derecho puede ocasionar la vulneración de los derechos a la intimidad, privacidad, imagen y honor del fallecido, además de limitaciones a los sucesores, como los ejemplificados en el ítem anterior.

Aquí también hay una crítica a la ya estudiada Ley argentina 26.529, de Derechos del Paciente en su Relación con los Profesionales e Instituciones de la Salud. Esta norma permite que terceros accedan a los datos contenidos en la historia clínica del paciente, sin establecer claramente los límites de este acceso. Según el artículo 19:

> Establécese que se encuentran legitimados para solicitar la historia clínica:

> a) El paciente y su representante legal;
> b) El cónyuge o la persona que conviva con el paciente en unión de hecho, sea o no de distinto sexo según acreditación que determine la reglamentación y los herederos forzosos, en su caso, con la autorización del paciente, salvo que éste se encuentre imposibilitado de darla;
> c) Los médicos, y otros profesionales del arte de curar, cuando cuenten con expresa autorización del paciente o de su representante legal.
> A dichos fines, el depositario deberá disponer de un ejemplar del expediente médico con carácter de copia de resguardo, revistiendo dicha copia todas las formalidades y garantías que las debidas al original. Asimismo podrán entregarse, cuando corresponda, copias certificadas por autoridad sanitaria respectiva del expediente médico, dejando constancia de la persona que efectúa la diligencia, consignando sus datos, motivos y demás consideraciones que resulten menester.

Existe una gran cantidad de personas autorizadas por ley para acceder a la historia clínica del paciente, entre ellas, los herederos forzosos. El permiso legal de acceso por parte de los herederos sin el establecimiento de límites o propósitos, hace que la intimidad y privacidad de una persona fallecida sea vulnerable a violaciones innecesarias de sus datos sensibles.

En Brasil, la sucesión digital no ha sido objeto de regulación ni en la Ley 12.965, del 23 de abril de 2014 –conocida como Marco Civil de la Internet que establece los derechos y garantías de los usuarios de la red–, ni en la Ley 13.709, del 14 de agosto de 2018 –que establece el régimen jurídico de protección de datos personales– (Font; Boff, 2019, pp. 48-49). Ninguna de estas reglas hace mención expresa al ejercicio de los derechos del titular de los datos personales por parte de sus sucesores, dejando aún más abierto a conflictos el tratamiento de los datos de un fallecido.

De la lectura de la Ley General de Protección de Datos Personales se puede concluir que el legislador centró su técnica en la figura del titular de la información. En este sentido Costa (2019, 3º párr.) sostiene que la LGPD es una ley que trae

normas y lineamientos para el tratamiento de datos personales, posicionando al titular de los datos como figura central.

Complementan a Beppu y Maciel (2020, p. 6), al decir que la intimidad-privacidad versada en la LGPD va más en la dirección de darle al titular el poder de decisión sobre qué datos se pueden utilizar o compartir, con quién y con qué finalidad, que para prohibir cualquier forma de compartir. Sin embargo, la regla olvida la finitud de esta figura, ya que no existe ninguna disposición en la ley que pueda relacionarse con la muerte del titular de los datos. Por esta razón, la interpretación de sus dispositivos debe ser extensa para poder probar un marco capaz de proteger al difunto del acceso indebido a sus datos.

En consecuencia, el principio de finalidad puede ser una alternativa al tratamiento de datos de una persona fallecida. La LGPD define este principio en el artículo 6, I, al establecer como finalidad la realización del tratamiento con fines legítimos, específicos, explícitos e informados al titular, sin posibilidad de ulterior tratamiento de forma incompatible con dichos fines. El artículo 15, I, por su parte determina que el cese del tratamiento de los datos personales se producirá, entre otras hipótesis, con la verificación de que se ha alcanzado la finalidad o que los datos ya no son necesarios o pertinentes para alcanzar la finalidad concreta que se busca.

Para Beppu y Maciel (2020, p. 7) el objetivo es tratar los datos con una finalidad legítima, específica, explícita e informada para el titular. En otras palabras, debe haber cumplimiento de la finalidad de tratamiento y transparencia con el titular. Este principio aparece en armonía con el de necesidad, que presupone la recogida proporcional de datos y el tratamiento mínimo necesario para lograr la finalidad informada.

Con la muerte del titular, las posibilidades de tratamiento de sus datos personales se reducen considerablemente, lo que requiere que el poseedor de los datos demuestre la persistencia de una finalidad, bajo pena de la obligación de suprimir la información. Pero existe la posibilidad de mantener el tratamiento de los datos, incluso después del fallecimiento del titular, precisamente por el interés

legítimo del controlador –nombre dado por LGPD al responsable del tratamiento de los datos personales–.

Beppu y Maciel (2020, pp.7-8) sostienen que esta hipótesis puede justificar el tratamiento realizado, salvo que prevalezcan los derechos y libertades fundamentales del titular y siempre que sea para fines legítimos, considerados desde situaciones concretas, como, por ejemplo, la protección del ejercicio regular de derechos del titular o prestación de servicios que le beneficien, respetando sus legítimas expectativas, derechos, y libertades fundamentales. En el caso de interés legítimo del controlador, el tratamiento debe limitarse a aquellos datos estrictamente necesarios para la finalidad prevista.

Al igual que con el principio de finalidad, existen otras disposiciones de la LGPD que pueden aplicarse en un intento de proteger los datos personales de un titular fallecido. Pero el esfuerzo realizado para implementar estas disposiciones deja en claro que la norma es insuficiente.

En efecto, según Beppu y Maciel (2020, p. 7), esto converge a la preocupación evidenciada en la LGPD, al establecer sus fundamentos y principios, con el fin de orientar las decisiones y modelos de conformidad (*compliance*), conscientes de que las situaciones específicas previstas en el texto normativo no son capaces de regular y predecir toda la serie de tratamientos, relaciones y arreglos contractuales, especialmente en vista de la velocidad tecnológica y la dinámica social, características de la fluidez del mundo contemporáneo.

La limitación ocasionada por la falta de regulación legal específica sigue siendo un obstáculo para el tratamiento del legado digital en Brasil. No obstante, la ley nacional de protección de datos establece pautas importantes para este tratamiento, a través de software y aplicaciones. Dado que la LGPD es la ley específica de protección de datos personales en el país, centralizará el sistema normativo en relación con esta materia, comenzando a orientar las decisiones judiciales y futuras normativas sobre el legado digital posterior a la muerte, y su tratamiento (Beppu; Maciel, 2020, p.11).

Aun así, además del carácter genérico antes mencionado y la incompletitud normativa de la LGPD, es necesaria la integración con otros estándares. Cabe

recordar que en los ítems 2 y 3 del capítulo II de este trabajo se estudiaron otras normas relacionadas con la protección de datos en Argentina y Brasil.

El Marco Civil de Internet es una de las normas brasileñas que, junto con la LGPD, puede aportar el mínimo de seguridad jurídica en el tratamiento de los datos personales de alguien que ya falleció. Ejemplo de ello es la garantía prevista en el artículo 7, III, de esta norma, que establece que el acceso a Internet es imprescindible para el ejercicio de la ciudadanía, garantizándose al usuario, entre otros, los derechos a la inviolabilidad y confidencialidad de sus comunicaciones privadas almacenadas, que solo se eliminarán por orden judicial.

En la misma línea, de acuerdo con el artículo 23 de la misma regla, el juez es responsable de tomar las medidas necesarias para garantizar la confidencialidad de la información recibida, y preservar la privacidad, la intimidad, el honor y la imagen del usuario, pudiendo determinar el secreto de justicia, incluidas las solicitudes de custodia del registro. La protección judicial es, por tanto, la que más eficazmente ha garantizado la protección de los datos personales en situaciones no reguladas por la norma.

Sin embargo, algunos proyectos de ley presentados en el Congreso Nacional de Brasil tienen como objetivo, el cambio de disposiciones del Código Civil, a fin de permitir expresamente la transmisión a los herederos de los derechos de los usuarios fallecidos relacionados con las redes sociales. Este es el Proyecto de Ley 4.847/2012, que se adjuntó al Proyecto de Ley 4.099/2012. Por caso, se observa el Proyecto de Ley 1.331/2015, que propone la modificación de la Ley del Marco Civil de Internet, con el fin de otorgar a los herederos la legitimidad para promover la exclusión de los datos del heredero fallecido (Maichaki, 2018, p.149).

Sobre este proyecto de ley, destacan Honorato y Leal (2020, p. 160), que buscó cambiar el inciso X del artículo 7 del Marco Civil, para determinar la legitimidad del cónyuge, ascendientes y descendientes para solicitar la supresión de los datos personales del usuario fallecido.

En el Proyecto de Ley 7.742, presentado en 2017, en opinión de Honorato y Leal (2020, p. 160), se sugirió, además, la inclusión del artículo 10-A al Marco Civil, para establecer que los proveedores de la aplicación deben excluir las

cuentas respectivas de los usuarios brasileños fallecidos, inmediatamente después de la prueba del fallecimiento, a solicitud del cónyuge, pareja o familiar, mayor de edad, obedeciendo la línea recta o colateral, hasta 2º grado. De acuerdo con la propuesta, las cuentas podrían mantenerse cuando esta opción fuera posible por el proveedor respectivo y si el cónyuge, pareja o familiar del fallecido realizara una solicitud al efecto, dentro de un año a partir de fallecimiento, quedando bloqueada la gestión por cualquier persona, salvo que el usuario fallecido hubiera dejado autorización expresa indicando quién debía gestionarlo.

Actualmente están archivadas todas las propuestas antes mencionadas. No obstante, el Proyecto de Ley 5.820/2019, en trámite, tiene como objetivo modificar el artículo 1.881 del Código Civil, con la inclusión de un párrafo 4 con la siguiente redacción: “Para la herencia digital, entendida como videos, fotos, libros, contraseñas de redes sociales, y otros elementos almacenados exclusivamente en la Internet, en la nube, el codicilo en video renuncia a la presencia de testigos para su vigencia”. También se encuentra en trámite el Proyecto de Ley 6468/2019 que, mediante la inclusión de un solo párrafo en el artículo 1.788 del Código Civil, pretende establecer la transmisión a los herederos de “todo el contenido de cuentas o archivos digitales propiedad del autor de la herencia” (Honorato; Leal, 2020, p. 160).

Argentina y Brasil no cuentan con una protección legal satisfactoria de los datos personales de las personas fallecidas en sus ordenamientos jurídicos; por lo tanto, son incapaces de garantizar una adecuada protección de la intimidad-privacidad *post mortem*, lo que confirma la hipótesis inicial de este trabajo. No obstante, esta realidad no es exclusiva de Argentina y Brasil, en la medida que los países latinoamericanos, como lo señalan Font y Boff (2019, p. 46), no regulan la disponibilidad de los datos personales luego del fallecimiento de su titular, de la misma forma que los Estados Unidos y Europa.

En orden a lo expuesto, se presentará una solución a la problemática objeto de estudio, partiendo de los paradigmas del Derecho Comunitario Europeo y de los Derechos español y francés. Previo a ello, se realizará un análisis sobre el

“Derecho al Olvido”, como guía momentánea para la protección de los datos, la intimidad, y privacidad de las personas fallecidas.

4 El “Derecho al Olvido” como guía para la protección de los datos y garantía de la intimidad y privacidad de las personas fallecidas en Argentina y Brasil

En primer lugar, se sugiere como una alternativa para paliar el fracaso legislativo en la protección de la intimidad, la privacidad y los datos de una persona fallecida, la figura jurídica del “Derecho al Olvido”. Su uso se configura como una solución temporal para garantizar la preservación de los derechos mencionados, hasta que la Argentina y Brasil protejan adecuadamente el tema en tratamiento.

Por otro lado, es una medida radical, ya que no permite el tratamiento de datos personales, en situaciones ya autorizadas por las leyes vigentes, como el interés legítimo del controlador de datos personales. En este ítem se hace un estudio más profundo sobre el “Derecho al Olvido” para entender cómo puede convertirse en una herramienta orientadora para la protección de los datos y de la intimidad-privacidad *post mortem.*

El “Derecho al Olvido” ha ocupado una amplia literatura mediática y jurídica durante el último lustro acompañando la explosiva omnipresencia de Internet en nuestras vidas y la incipiente demanda de cancelación de datos personales en la red ante el temor de que pudieran perjudicar en el futuro la imagen, privacidad y reputación individual (Rallo, 2016, p. 19).

En este mismo sentido, Viola, Doneda, Córdova e Itagiba (2016, p. 65) observan que la reciente demanda de “Derecho al Olvido” se puede ver en el contexto de reordenamiento de poderes que brinda la facilidad de almacenamiento y acceso a la información, características de la Sociedad de la Información.

En este contexto surge la necesidad de dotar de alguna herramienta legal que permita solucionar la situación, más de las veces injusta, por la que atraviesa

quien aparece vinculado actualmente a una información antigua y negativa sobre su persona, y que lo transforma, en los hechos, en prisionero de su pasado. Esta herramienta, precisamente, es el denominado “Derecho al Olvido”, respecto de aquellas informaciones que en una época fueron publicadas lícitamente, pero que con el transcurrir del tiempo perdieron vigencia, causando en el presente un daño desproporcionado con su publicación, razón por la cual ameritan ser objeto de un tratamiento limitado o derechamente eliminadas. Juegan aquí las nociones de tiempo, memoria, perdón, rehabilitación, desarrollo de la personalidad y plan de vida (Puccinelli, 2019, p. 80).

En cuanto a la nomenclatura de este derecho, Diniz (2017, p. 11), afirma que, según la doctrina francesa, parece que lo correcto sería decir el derecho de ser olvidado y no el “Derecho al Olvido”, porque nadie puede ser obligado a olvidar ni puede imponer a la comunidad el deber de olvidar. A pesar de esta comprensión, como se observará a continuación, gran parte de la doctrina utiliza el término “Derecho al Olvido”, por lo que esta es la forma elegida en la redacción de esta tesis.

Existe cierta controversia en torno al citado instituto. En la lección de Retondo (2016, pp. 85-86), este derecho condice con una necesidad humana, en muchos casos, de olvidar para cambiar y evolucionar. Pero también para esto suele ser necesario, y la determinación de “Derecho al Olvido” aparece, entonces, con una connotación que no corresponde, la de pretender alterar la realidad u oponerse al “Derecho a la Verdad”, en especial en temas de alto interés público.

En consonancia con lo expuesto, Puccinelli (2019, p. 89) sostiene, que parece claro que ni una admisión sin limitaciones ni una negación absoluta son soluciones apropiadas, y por ello debería ser reconocido universalmente, pero de manera limitada y bajo una ponderación caso por caso donde sólo se lo reconozca respecto de informaciones sobre las que no existe un interés público relevante que predomine sobre ese derecho, a que sean expurgadas de la memoria colectiva.

El debate sobre el denominado “Derecho al Olvido” o “a ser olvidado” parte de las nociones del tiempo y la memoria y se vincula expresamente con los hechos pasados –esto porque más allá de que ciertos hechos que puedan ser

registrados refieran a momentos recientes y mantengan actualidad porque están desarrollándose o de que pueda especularse con hechos futuros, los sistemas de información sólo recopilan hechos pertenecientes al pasado–, donde en la dimensión humana –a diferencia de lo que ocurre en el ámbito informático–, el flujo del tiempo va paralela y gradualmente desdibujando los hechos percibidos y agotando su relevancia social o su potencial informativo hasta el punto en que ellos ya no merecen ser colectivamente memorados (Puccinelli, 2019, pp. 78-79).

En el mismo sentido Rallo (2016) advierte:

> [E]l debate sobre el derecho al olvido en Internet nada tiene que ver con el fin de la memoria, con prescindir del pasado, con el falseamiento de la historia o con la supuesta instauración de un filtro censor universal al ejercicio del derecho a la información. [...] Ni la memoria individual ni la historia colectiva están –ni pueden estar– en juego porque Internet depure específicas informaciones personales relativas a individuos que ni tienen ni pretenden gozar de interés público alguno. Porque la condición de uso de Internet ni es ni puede ser la publicidad universal de cualquier dato personal que en ella se vuelque. Porque la memoria individual sobre informaciones propias podría constituir derecho subjetivo pero el recuerdo sobre los datos ajenos de ciudadanos anónimos tendrá el calificativo que merezca, pero nunca el derecho a preservar la integridad de la historia. Porque el derecho a saber y a estar informados alcanza sin matices a todo asunto de interés general pero no a cualquier dato personal que voluntariamente o no haya sido hecho público por un particular en el marco de sus relaciones personales y sociales. (p. 20).

Sobre la construcción jurisprudencial, Remolina Angarita (2017, p. 200) aclara que ha comprendido el análisis de varios derechos y principios. Dentro de los primeros se mencionan, entre otros, la intimidad, la protección de datos personales, el buen nombre, la libertad de expresión, el derecho a informar y recibir información. Dentro de los segundos, se encuentran el principio de la dignidad humana y la neutralidad tecnológica de internet.

En Brasil, la controversia sobre la aplicabilidad del “Derecho al Olvido” ganó nuevos contornos después de la sentencia del Supremo Tribunal Federal en el recurso extraordinario 1010606, que estableció la siguiente tesis:

> Es incompatible con la Constitución la idea de un derecho al olvido, entendido así como la facultad de impedir, por el paso del tiempo, la divulgación de hechos o datos veraces y lícitamente obtenidos y publicados en medios de comunicación analógicos o digitales. Los excesos o abusos en el ejercicio de la libertad de expresión e información deben ser analizados caso por caso, con base en parámetros constitucionales -especialmente los relativos a la protección del honor, la imagen, la privacidad y la personalidad en general- y las expresas y específicas disposiciones legales en los ámbitos penal y civil. (STF. Tribunal Pleno. RE 1010606/RJ, juzgado en 11/02/2021, Tema 786)

Se advierte que esta decisión no cierra la discusión, ya que se trata específicamente de la aplicación del “Derecho al Olvido” en una situación de divulgación de hechos o datos veraces y legalmente obtenidos y publicados en medios de comunicación analógicos o digitales. Es evidente que existen casos de información que aún no ha sido publicada o accedida por terceros, como las almacenadas en proveedores de internet o cuentas de redes sociales. Estos casos también deben ser confrontados con el derecho en foco para evaluar la viabilidad de su aplicación. Como explica Remolina Angarita (2017, p. 200) el reconocimiento del “Derecho al Olvido” es principalmente casuístico. Los hechos reales y las situaciones concretas han sido determinantes para el reconocimiento y garantía del mismo.

Dicha discusión está íntimamente relacionada con la protección de los datos personales, ya que son ellos quienes portan la información que se pretende olvidar. Por ello, la temática cobró intensidad en 2010, cuando, según Rallo (2016, p. 23) la Comisión Europea presentó en Bruselas la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre “Un enfoque global de la protección de los datos personales en la Unión Europea” en la que por primera vez se hacía referencia

explícita al “Derecho al Olvido” en un documento oficial de las instituciones europea.

Aún para Rallo (2016, p. 25) la Comunicación de la Comisión Europea evidenciaba el nacimiento del concepto de olvido ligado al entorno digital online y, especialmente, a las redes sociales.

Los derechos que se reconocen a los titulares de los datos en las normas que regulan el derecho a la protección de los datos personales, vinculados directamente con el “Derecho al Olvido”, son tres: de acceso; cancelación (o supresión), y de oposición al tratamiento de los datos personales (Puccinelli, 2019, p. 80). En un sentido similar, Remolina Angarita (2017, p. 216) defiende que, frente a la falta de definición universal del “Derecho al Olvido”, este no solo es el clásico derecho de eliminación de información, sino que guarda relación con el derecho de oposición que permite a las personas que en excepcionales circunstancias solicite la eliminación negativa y verdadera de su pasado.

De acuerdo con Puccinelli (2019, p. 80) algunos autores (e incluso la versión de 2012 del actual Reglamento General de Protección de Datos de la Unión Europea) ubican al “Derecho al Olvido” exclusivamente dentro del derecho de cancelación de datos personales vetustos (los que ya no cumplen con la finalidad para la cual fueron recabados, dado que ofrecen un perfil desactualizado de la persona a la que refieren).

Es el caso de Retondo (2016, p. 89) que defiende, en términos más generales, que, en virtud de la existencia del derecho a la supresión, que se apoya en la oposición al tratamiento por parte del titular y es parte natural del complejo que configura la protección de datos personales, el “Derecho al Olvido” aparece en su desarrollo, en el entorno tecnológico, en el cual la información se expande espacial y temporalmente en grado sumo y afecta lo que se ha llamado, la “reputación online”.

Esta perspectiva no es del todo correcta porque por más que siempre hay algo que se suprime -por ejemplo, un vínculo- también puede ser visualizado como una excepción al derecho de acceso a datos que no deben ser cancelados o puede ejercerse a fin de que el titular de los datos impida, vía oposición, que un

dato sea objeto de determinados tratamientos, en ambos casos, sin que ello necesariamente implique su cancelación (Puccinelli, 2019, p. 80).

El Reglamento General de Protección de Datos Europeo trata expresamente el derecho a la supresión como el “Derecho al Olvido”. En el considerando 66, el texto contiene la siguiente disposición:

> [A]fin de reforzar el derecho al olvido en el entorno en línea, el derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos. Al proceder así, dicho responsable debe tomar medidas razonables, teniendo en cuenta la tecnología y los medios a su disposición, incluidas las medidas técnicas, para informar de la solicitud del interesado a los responsables que estén tratando los datos personales.

En el artículo 17 del RGPD, se regula el “Derecho al Olvido” como derecho a la supresión. En el referido dispositivo se señalan las circunstancias en que el interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan. Entre estas circunstancias se encuentran la extinción de la finalidad en el tratamiento de datos, la retirada del consentimiento y el ejercicio del derecho de oposición.

En palabras de Luz (2019, pp. 196-197), el Reglamento General Europeo de Protección de Datos dedica todo un artículo (artículo 17) sobre el “Derecho al Olvido”, apuntando desde las posibilidades de aplicación (artículo 17, 1), requisitos técnicos para los responsables del tratamiento de los datos –para la realización de este derecho– e incluso hipótesis restrictivas para su aplicación (artículo 17, 3). Entre tales restricciones, se encuentra la comparación con la libertad de expresión y el derecho a la información, la protección de datos para fines de cumplimiento de las instituciones públicas, la garantía del interés público, la protección de los hechos científicos, la investigación histórica, la estadística y, finalmente, el ejercicio de la defensa judicial.

En el caso de Argentina y Brasil, se ha dicho repetidamente que los respectivos sistemas de protección de datos personales están extremadamente

influenciados por el sistema de regulación europea. La diferencia radica en que Argentina aún no ha aprobado su nueva Ley de Protección de los Datos Personales, proyecto que ingresara al Congreso Nacional hace algunos años. Sin embargo, Keller (2017, p. 173) advierte que los recientes avances europeos en materia jurídica respecto del llamado “derecho al olvido” no encuadran correctamente con el marco jurídico y de derechos humanos de América Latina.

Juri (2019, p. 229) explica, que a pesar de no contemplar el “Derecho al Olvido”, la ley argentina vigente considera casos en donde el usuario puede solicitar que se borren contenidos falsos o inexactos; por ejemplo, a través del artículo 16 -Derecho de rectificación, actualización y supresión-. Mientras que el artículo 17 plantea excepciones, pues los responsables o usuarios de bancos de datos pueden denegar el acceso, rectificación o la supresión del contenido, "en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros".

En la misma línea, también cabe mencionar lo establecido en el artículo 26, inciso 4, de la Ley Argentina de Protección de Datos Personales, que trata de la prestación de servicios de información crediticia:

> Sólo se podrán archivar, registrar o ceder los datos personales que sean significativos para evaluar la solvencia económico-financiera de los afectados durante los últimos cinco años. Dicho plazo se reducirá a dos años cuando el deudor cancele o de otro modo extinga la obligación, debiéndose hace constar dicho hecho.

Vale recordar que el artículo 43, tercer párrafo de la Constitución Argentina ya regulaba el derecho de supresión y que el proyecto de la nueva ley argentina de protección de datos personales contempla este derecho de manera más amplia, como se pudo observar en los capítulos anteriores.

En el caso de Brasil, según Luz (2019, p. 197), la Ley General de Protección de Datos Personales no utiliza específicamente el término “Derecho al Olvido”, aunque sí determina la exclusión de los datos una vez finalizado su tratamiento, planteando dos hipótesis principales: la pérdida de la finalidad específica deseada con los datos y el ejercicio de revocación del consentimiento (artículos 15 y 16).

Resaltando el principio de finalidad, ya estudiado en el ítem anterior de este capítulo, Luz (2019, p. 198) sostiene que este principio, confirmado en la legislación nacional brasileña, tiene una notoria relación con el llamado “Derecho al Olvido” en Internet, pero eso no es precisamente su consagración; si bien resulta posible, que futuras decisiones sobre el tema se inspiren en éste y otros principios de la Ley General de Protección de Datos, ya que la respuesta a los conflictos en esta materia, no encuentra en las normativa vigente, una vía segura para su solución.

Aún sobre la LGPD, Luz (2019, p. 199) sostiene que no es posible conocer de antemano los efectos futuros, y si sus principios de hecho serán tenidos en cuenta y bien ponderados por los operadores de la ley. Su innegable virtud es enfatizar ante los ciudadanos la importancia de una cultura positiva en la protección de la personalidad humana, en general, y en los datos personales, en particular, reavivando la discusión de temas como el consentimiento, la intimidad-privacidad y el valor de la información.

Diniz (2017, p. 12) asegura que la única mención expresa en el ordenamiento jurídico brasileño, del derecho de ser olvidado, se encuentra en el Marco Civil de Internet; cuyo artículo 7, X, establece:

> Art. 7º. O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: [...] X – exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta lei.

Ni Argentina ni Brasil adoptan expresamente la nomenclatura del “Derecho al Olvido” en sus ordenamientos jurídicos, lo que no significa que no exista una normatividad. Los derechos de exclusión, supresión, oposición y otros son suficientes para garantizar al individuo una base jurídica para el ejercicio del “Derecho al Olvido”. Hasta las mismas bases constitucionales y de derechos humanos pueden utilizarse para garantizar ese derecho. En este sentido, en la lección de Diniz (2017, p. 13), el “Derecho al Olvido” es un derecho de la

personalidad y es un derecho fundamental basado en la dignidad de la persona humana.

Keller (2017, p. 198) sugiere que fundamentar el derecho al olvido en una ley de protección de datos similar a la de la UE conduce al desequilibrio en las reglas, que dejan sin protección suficiente a los derechos de libertad de expresión de los usuarios de Internet. Una posible solución en la UE y en otras partes sería incorporar nuevas e importantes protecciones sustantivas y procedimentales a la expresión dentro de la Ley de Protección de Datos.

En cuanto a la protección de la intimidad y privacidad *post mortem*, ejercida a través del "Derecho al Olvido", especialmente de los datos de la persona fallecida, tampoco existe consenso. Silva *et al* (2020, p. 378) afirman que la herencia digital –donde se incluyen los datos personales del fallecido, de acuerdo con lo expuesto en el ítem 2 de este capítulo– y el "Derecho al Olvido" se han discutido desde los límites entre lo público y lo privado y los derechos individuales inherentes a la dignidad de la persona humana, como la intimidad, el honor y la privacidad. También existe el derecho a la información y la libertad de expresión.

En este sentido, el "Derecho al Olvido" está íntimamente relacionado con la garantía de privacidad, lo que entra en conflicto con la libertad de expresión. A pesar de tener el objetivo de proteger la privacidad de las personas, afecta, en particular, los datos personales que, en la práctica, debido a los nuevos valores que aporta la tecnología, reflejan la privacidad de los datos digitales. En definitiva, es un derecho que también está relacionado con los contenidos de Internet y fruto de su disponibilidad (Silva; *et al*, 2020, p. 379).

Critico del "Derecho al Olvido", Bertoni (2014, párrafo 9) explica que si por un lado, jueces y legisladores, quizás sin considerar exhaustivamente las consecuencias, "ven" en este derecho la necesidad de proteger la privacidad; por otro lado, los defensores de la libertad de expresión, el acceso a la información y la búsqueda de la verdad "ven" sus desventajas.

Para Bertoni (2014, párrafo 9), cuando las personas se sientan perjudicadas por la información disponible sobre ellos en línea, deberían poder impugnar esta información directamente, y el propio motor de búsqueda debe tener un

instrumento que permita este proceso. Más información, no menos. De esa forma, podria dejar de discutirse el “Derecho al Olvido”, que está equivocado en muchos aspectos, incluso por su nombre ofensivo.

Una alternativa propuesta por Bertoni y Cortés Castillo (2014, p. 148) son las fechas de vencimiento de datos o de etiquetas personales, que apuntan a un desarrollo tecnológico que no debe pasar desapercibido. Ya sea a través de mecanismos legales o de autorregulación, ideas como estas podrían servir para abordar la propuesta de una especie de “Derecho al Olvido” que preserve el equilibrio de los derechos humanos involucrados.

A raíz de esta colisión de derechos, Texeira y Paula (2017, p. 43) recuerdan que un usuario fallecido no necesariamente querría que sus correos electrónicos fueran vistos por su familia, para mantener su privacidad e incluso su reputación, porque el correo electrónico es, por regla general, personal, y solo el usuario accede a la información contenida en él, a diferencia de un perfil en una red social, donde las publicaciones son públicas y pueden ser vistas por otros.

Por ello, defienden Silva, *et al*, (2020, p. 383) que es necesario pensar en mecanismos que aseguren el derecho a la privacidad de los datos personales, permitiendo al usuario decidir y elegir la mejor forma de compartir su información, sea en actividad, sea en inactividad.

El “Derecho al Olvido” es uno de estos mecanismos. La persistencia del perfil y de la personalidad digital del fallecido en el mundo virtual requiere medios efectivos para la protección de los derechos de la personalidad, como el derecho a la privacidad. En ausencia de normas que delimiten y resuelvan los conflictos entre derechos relacionados con los datos personales, el derecho a ser olvidado es una alternativa de protección jurídica momentánea. Así, hasta que la ley regule satisfactoriamente la materia, el olvido de los datos de la persona fallecida puede ser una guía para la protección de la intimidad y privacidad *post mortem*.

Por otro lado, la aplicación del “Derecho al Olvido” para proteger los datos personales y la intimidad-privacidad de una persona fallecida no pueden darse de manera indiscriminada, precisamente por la existencia de otros derechos a mitigar, como ya se destacó. El análisis del caso específico debe orientar si es apropiado o

no hacer uso de ese derecho. Idealmente, tal análisis debería ser realizado siempre por una autoridad judicial, pero, en la imposibilidad, los propios titulares de los datos personales y los sucesores del fallecido deberían sopesar la viabilidad del derecho de no ser recordado.

Para Texeira y Paula (2017, p. 43), los familiares y/o herederos están calificados para tomar cualquier decisión sobre la colección digital dejada por el *de cujus*, y cuando el patrimonio es meramente sentimental y sin valores económicos, tienen derecho a requerir la desvinculación o cancelación de cuentas o expedientes que puedan circular en medios electrónicos relacionados con el difunto y que provoquen daño emocional o trastorno psicológico a la familia para que, así, el dolor y sufrimiento no continúe en el tiempo.

Pero advierten Manchini, Augusto y Franceschet (2020, p. 101), que, en ausencia de una disposición en vida por parte del fallecido sobre el destino de la herencia afectiva, los herederos y sucesores no podrán acceder a las cuentas sociales del *de cujus*, bajo pena de atentar contra sus derechos fundamentales y personalidad, debiendo prevalecer lo dispuesto en la aceptación del uso de la red social, que, en su mayoría, establece la desactivación automática del perfil en caso de fallecimiento, sin, no obstante, permitir el acceso a terceros.

De esta forma, el “Derecho al Olvido” se utilizaría independientemente de la voluntad de los sucesores del fallecido, que parece ser el ideal. Así, con el paso del tiempo, sin acceso a datos personales, se producirá un olvido natural de la información protegida por la intimidad-privacidad.

Sin embargo, en la opinión de Remolina Angarita (2017, p. 224), el “Derecho al Olvido” ha cobrado especial relevancia frente a publicaciones en Internet de hechos verdaderos del pasado de las personas, que ahora, por motivos particulares de los afectados, desean que se suprima definitivamente. Al mismo tiempo, el ciberespacio es el contexto en donde principalmente tienen lugar dichas situaciones, lo cual hace muy difícil lograr que se materialice efectivamente el “Derecho al Olvido” en dicho escenario digital, transfronterizo e incontrolable tanto por la cantidad de cibernautas, como por el diseño de red global, abierta y de fácil acceso que tiene Internet.

En definitiva, lo que se concluye es que el “Derecho al Olvido” es un medio eficaz para proteger los derechos de la personalidad *post mortem* y no debe, por regla general, aplicarse a todo el conjunto de datos personales de la persona fallecida, sino únicamente a aquellos que no tienen valor económico, generados en un contexto de la vida privada del fallecido. No obstante, en el caso de datos personales que tengan valor económico, al portar información privada sobre el fallecido, se recomienda el uso del “Derecho al Olvido”, al menos, hasta que exista una adecuada protección estatal.

5 Conclusión

La finitud es algo que llegará a todas las personas, indiscriminadamente, siendo la muerte el evento más democrático del planeta. Nadie, aún, puede escapar a tal resultado. La prolongada longevidad y, hasta la misma inmortalidad rondaron por siglos en las mentes fértiles del ser humano con el objeto de eternizar la vida; si bien, ninguna tecnología, por avanzada y disruptiva que sea, logró concretar dicho objetivo. En algunos casos, la ciencia prolonga la vida; si bien es sabido que el final siempre es el mismo.

En este capítulo se presentaron algunos intentos de camuflar el fin humano, dejando muy claro que son solo meras soluciones tecnológicas que ni siquiera están cerca de poder acercarse a la longevidad o la inmortalidad. De hecho, estas soluciones son objeto de la ansiedad que algunos tienen por superar la muerte; mecanismos que sirven solo de consuelo para los que se quedan.

Las herramientas aquí presentadas no son más que medios tecnológicos para transferir información –datos– de la persona fallecida a terceros. Él, el muerto, en efecto, se marcha con finitud, llevándose consigo sus sentimientos, su conciencia y su vida. Lo que queda son los datos de la persona, que no pueden portar tales atributos.

No por eso, estos datos, que adquieren el estatus de bienes digitales en la sociedad de la información, merecen ser descuidados. Tienen su importancia económica y merecen ser reguladas por la ley de sucesiones. Pero también tienen

una importancia personal, ya que llevan la historia y las huellas de las acciones de la persona fallecida.

El acceso inadecuado a este tipo de datos puede denigrar la memoria del fallecido y su familia. En este caso, el derecho de sucesión no es capaz de proteger la transferencia de información a sucesores y terceros por sí solo. La protección de los derechos de la personalidad no es igualmente eficaz para garantizar la protección de la intimidad y la privacidad cuando se procesan los datos personales del fallecido.

Es entonces cuando el tema de la protección de datos personales adquiere una importancia considerable para garantizar la inviolabilidad de la intimidad-privacidad *post mortem*. Estrechamente ligado a cuestiones tecnológicas, el sistema de protección de este tipo de patrimonio digital puede, junto con otros derechos, garantizar el adecuado tratamiento de los datos que deja el fallecido, sin tener acceso a lo que no quiso publicar.

Por tal motivo, se realizó un análisis de los sistemas jurídicos de protección de datos personales en Argentina y Brasil para comprender el nivel de protección de la intimidad y privacidad garantizado a los fallecidos por ambos países. La conclusión fue la confirmación de la hipótesis inicial planteada en la introducción de este trabajo, ya que se encontró que ninguna de las naciones estudiadas cuenta con sistemas de protección de datos personales capaces de garantizar la intimidad-privacidad de una persona fallecida. Luego, no existe suficiente protección jurídica adecuada a la situación descrita. Pero eso no significa que no existan reglas al respecto.

En ambos países, la legislación vigente cede a los herederos y sucesores la legitimidad para la defensa de los derechos de la personalidad, lo que se refleja en el tratamiento de los datos personales. Derechos como el derecho de acceso, oposición y supresión, así como la exigencia de cumplir con principios como la finalidad, garantizan a los datos personales del fallecido un mínimo de protección legal. Pero en relación a la intimidad y privacidad *post mortem*, tales derechos y principios no son suficientes para garantizar una regulación adecuada.

Las leyes vigentes, y aquellos proyectos de ley que se están analizando en las cámaras legislativas de Argentina y Brasil, no se preocupan por el hecho de que permitir el acceso a los datos personales de una persona fallecida significa poner en riesgo su intimidad-privacidad y otros derechos de la personalidad *post mortem*.

Así las cosas, las decisiones sobre garantizar o no el conocimiento del contenido de los datos personales del difunto, quedan bajo la responsabilidad de los titulares de los datos o del poder judicial. Al parecer, el asunto seguirá, de forma temporal, sin una adecuada estandarización, lo que exige un gran esfuerzo por parte de los involucrados en el tratamiento de los datos del fallecido para tomar la decisión correcta.

Un norte está en el “Derecho al Olvido”. Se analizó que este Derecho puede ser una barrera efectiva para la violación de la intimidad y privacidad de una persona fallecida. Su aplicación asegura que, en el caso de datos personales que contengan información del ámbito privado de la persona fallecida, no existan accesos y restricciones indebidos.

De manera indirecta, el “Derecho al Olvido” ya ha sido utilizado por algunas redes sociales, que no permiten, bajo ningún concepto, el acceso a información de la cuenta, como conversaciones, imágenes, escritos o sonidos. Con esto, el transcurso del tiempo hará que se olviden las acciones realizadas por el fallecido en sus perfiles, estableciendo así el “Derecho al Olvido”.

Pero el citado instituto no debe ser aplicado en todas las situaciones; no resultando apropiado, cuando los datos del fallecido tienen un valor meramente económico. En este caso, el derecho sucesorio debe ser el encargado de promover la transmisión a los herederos, cuidando siempre de garantizar la intimidad-privacidad *post mortem*. También existe información pública sobre el fallecido, que refleja su historia y legado, y no es igualmente apropiado hacer uso del “Derecho al Olvido” en tales situaciones.

Lo privado debe seguir siendo privado, a menos que el titular exprese la intención de hacerlo público. Después del fallecimiento, se debe seguir respetando esta regla y, si no hubo manifestación previa de interés en la publicación, se

deben olvidar los datos personales, especialmente aquellos que pongan en riesgo la intimidad y privacidad, al menos, hasta que la ley encuentre una forma efectiva de permitir el tratamiento, sin ninguna violación de ningún derecho de la personalidad.

Capítulo V: Propuesta jurídica para salvaguardar la utilización de los datos de las personas fallecidas guardados en Internet en Argentina y Brasil

Existe una gran expectativa de que los países de América Latina intensifiquen en los próximos años la adecuación de las legislaciones nacionales relacionadas con los avances tecnológicos. Los motivos son los más variados, pero la necesidad de adaptarse a los estándares internacionales tiene un fuerte peso.

La gran dificultad radica en que los temas que involucran tecnología no se limitan a un territorio, lo que obliga a las naciones a normatizar siguiendo un modelo de estándar de otros países o comunidades de países. Este es el caso de la protección de datos personales, que encontró en el Reglamento General de Protección de Datos Europeo la norma estándar que inspira leyes sobre la materia, a nivel mundial.

Afirman López, Maranhão, Campos y Abrusio (2020, párr. 2) que, desde que entró en vigor el Reglamento General de Protección de Datos Personales Europeo (RGPD), en 2018, la adecuación a la protección de datos personales puede percibirse como un verdadero requisito del mercado. Para parte de las empresas, la gobernanza de la protección de datos ya era un problema de mercado que les permitiría una ventaja competitiva y una condición para la supervivencia. Esto se debe a que las empresas sujetas a la normativa europea empezaron a exigir garantías a sus socios y proveedores sobre su nivel de adecuación.

Argentina y Brasil se encuentran entre los países que se inspiran en el Reglamento Europeo para adaptar sus leyes de protección de datos personales. Pero en el caso de datos de personas fallecidas, no se observa que hubo la misma inspiración.

La respuesta es simple, el RGPD incluye en el considerando 27 la disposición de que la norma comunitaria no se aplica a la protección de datos personales de personas fallecidas y que los Estados miembros son competentes

para establecer normas relativas al tratamiento de los datos personales de estas. La inaplicabilidad también se recuerda en los considerandos 158 y 160.

Varios Estados miembros de la UE (Bulgaria, República Checa, Dinamarca, Estonia, Francia, Italia, Letonia, Lituania, Portugal, Eslovaquia, Eslovenia y España) han establecido un Reglamento para la protección de datos *post mortem* en diferentes formas, mientras que pocos Estados miembros excluyen explícitamente esta protección (Seminario, 2020, párr. 33).

En España, el Rey Felipe VI sancionó, el 5 de diciembre de 2018, la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales. Al igual que ocurre con el Reglamento General, la ley española no se aplica a los datos personales del difunto, por disposición expresa en el artículo 2.2, b. Aun así, la norma proporciona una orientación importante sobre el tema, especialmente en los artículos 3 y 96.

Dicho artículo 3 dispone lo siguiente:

> [A]rtículo 3. Datos de las personas fallecidas.
> 1. Las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión.
> Como excepción, las personas a las que se refiere el párrafo anterior no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los datos de carácter patrimonial del causante.
> 2. Las personas o instituciones a las que el fallecido hubiese designado expresamente para ello podrán también solicitar, con arreglo a las instrucciones recibidas, el acceso a los datos personales de este y, en su caso su rectificación o supresión.
> Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de estos mandatos e instrucciones y, en su caso, el registro de los mismos.
> 3. En caso de fallecimiento de menores, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus

> competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.
> En caso de fallecimiento de personas con discapacidad, estas facultades también podrán ejercerse, además de por quienes señala el párrafo anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo, si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

Téngase en cuenta, en el párrafo 1 del artículo, que se otorga permiso legal para acceder a datos personales para personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos. En este punto Fernandéz (2020, p. 72) aclara que se indica en el precepto que serán las personas que tengan una vinculación con el fallecido, y distingue la vinculación de naturaleza familiar (padres, cónyuge, hijos, nietos, etc.) o de hecho (pareja de hecho), así como sus herederos.

Si, en efecto, la legitimación para ejercerlos descansara únicamente en la persona que el fallecido hubiera designado a tal efecto, no se plantearía ningún problema de colisión con el derecho a la intimidad pretérita de este individuo. Sin embargo, el legislador español ha decidido consagrar una legitimación muy amplia que incluye a cualquier persona vinculada con el fallecido, por razones familiares o de hechos. Piénsese en lo inadecuado –y lesivo– que podría resultar que cualquier pariente de la persona fallecida pudiera solicitar de una red social o a una organización determinada el acceso a los datos personales que hubieran sido facilitados por aquellas para abrir su perfil o acceder a la membresía de esa organización (Imbernón, 2020, p. 249).

Aún acerca del artículo, Seminario (2020, párr. 45-46) destaca que, cuando el fallecido sea menor de edad, podrá realizarse este tratamiento en los supuestos indicados anteriormente, además por sus representantes legales y/o el Ministerio Fiscal quien actuará de oficio o a instancia de cualquier persona física o jurídica interesada. En caso de ser una persona con discapacidad, pueden realizar esas solicitudes las personas designadas como sus representantes, siempre que esas

facultades se encuentren incluidas en las medidas de apoyo prestadas por el designado.

Los derechos garantizados por la legislación española son los derechos de acceso, rectificación o supresión de los datos de la persona fallecida. Al igual que en la Ley de Protección de los Datos Personales de Argentina, la normativa española no limita el ejercicio de los derechos antes mencionados.

Por lo tanto, no garantiza que no habrá un acceso ilimitado al contenido de los datos personales, poniendo en peligro la protección de la intimidad, de la privacidad y de otros derechos de la personalidad del titular fallecido. Un mecanismo de limitación es la posibilidad de prohibir el ejercicio de los derechos de acceso, rectificación y supresión por voluntad previa expresa del interesado o por disposición legal.

El mecanismo de limitación en foco deja una apertura al acceso al contenido de los datos personales del fallecido, que es el desconocimiento de la prohibición de acceso, rectificación o supresión dejada por el fallecido, cuando los datos sean de carácter patrimonial.

Sobre la prohibición dejada por el difunto, Fernandéz (2020, p. 77) indica que sobre el precepto que sea, no es admisible una prohibición tácita, ni tampoco una indicación que no resulte de forma clara la prohibición y genere dudas. Igualmente, ello no es óbice para que los herederos puedan ejercer su derecho de acceso a datos patrimoniales, no personales del causante, a efectos de conocer el alcance patrimonial del mismo para el reparto de la herencia.

Aquí se hace una crítica a esta permisividad. Como ya se ha dicho en este trabajo, incluso en el caso de datos personales de importancia económica, existe un gran riesgo de vulneración de la intimidad-privacidad *post mortem* si existe un permiso de acceso indiscriminado para la satisfacción de los derechos patrimoniales de los herederos. En tal situación, debe haber un análisis previo del riesgo de acceso al contenido de los datos personales y también una ponderación de los derechos, con el fin de garantizar los derechos hereditarios de los sucesores y personalidades del fallecido.

También en la Ley de Protección de Datos Personales y garantía de los derechos digitales de España, el artículo 96 dispone sobre la posibilidad de acceso a los datos de una persona fallecida. Para Fernandéz (2020, p. 73) bajo la denominación del erróneo concepto que intitula el artículo 96 de la Ley Orgánica 3/2018 como Derecho al testamento digital, regula el acceso a contenidos gestionados por prestadores de servicios de la sociedad de la información sobre personas fallecidas.

Según Fernandéz (2020, p. 79), "testamento digital" es un concepto completamente desafortunado, ya que el testamento digital no existe en el ordenamiento jurídico de España. Completa Imbernón (2020, p. 254) diciendo, que los contenidos digitales a los que se refiere la norma del artículo 96 no siempre constituyen bienes transmisibles que puedan ser objeto de una sucesión *mortis causa*, lo que alejaría esta regulación del ámbito del Derecho hereditario, que solo abarca aquellos bienes y derechos que lo sean.

La sistemática del artículo 96 de la Ley Orgánica 3/2018 es similar a la planteada en el artículo 3 ya estudiado, estando ahora regulado el acceso a los contenidos de los proveedores de servicios digitales a los efectos sucesorios. De acuerdo con el artículo en foco (párr. 1) el acceso a contenidos gestionados por prestadores de servicios de la sociedad de la información sobre personas fallecidas se regirá por las siguientes reglas:

> [a)] Las personas vinculadas al fallecido por razones familiares o, de hecho, así como sus herederos podrán dirigirse a los prestadores de servicios de la sociedad de la información al objeto de acceder a dichos contenidos e impartirles las instrucciones que estimen oportunas sobre su utilización, destino o supresión.
> Como excepción, las personas mencionadas no podrán acceder a los contenidos del causante, ni solicitar su modificación o eliminación, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los contenidos que pudiesen formar parte del caudal relicto.
> b) El albacea testamentario, así como aquella persona o institución a la que el fallecido hubiese designado expresamente para ello también podrá solicitar, con arreglo a las instrucciones recibidas, el acceso a los

> contenidos con vistas a dar cumplimiento a tales instrucciones.
> c) En caso de personas fallecidas menores de edad, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.
> d) En caso de fallecimiento de personas con discapacidad, estas facultades podrán ejercerse también, además de por quienes señala la letra anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

Los legitimados se podrán dirigir a los prestadores de servicios de la sociedad de la información para acceder a los contenidos e indicarles las instrucciones que estimen convenientes sobre la utilización, destino o supresión de los contenidos allí alojados (Fernandéz, 2020, pp. 75-76). De acuerdo con el párrafo 2° del artículo 96 ahora analizado, tales personas podrán decidir acerca del mantenimiento o eliminación de los perfiles personales de personas fallecidas en redes sociales o servicios equivalentes, a menos que el fallecido hubiera decidido acerca de esta circunstancia, en cuyo caso se estará a sus instrucciones.

Aquello que todas estas personas pueden realizar respecto de los contenidos digitales, son los siguientes: a) mantener el perfil personal de la persona fallecida en las redes sociales o servicios equivalentes; b) eliminar el perfil personal de la persona fallecida en las redes sociales o servicios equivalentes (Fernandéz, 2020, pp. 76).

Hay que tener en cuenta que la decisión que se tome será siempre y cuando la persona fallecida no hubiera decidido sobre ello. En el caso de que haya procedido a indicar algunas instrucciones, se atenderá a ellas (Fernandéz, 2020, pp. 77).

Sobre el artículo en debate, se observa, que también es posible que el fallecido prohíba el acceso a los contenidos en poder de los proveedores de servicios. Recuerda Fernandéz (2020, p. 76) que esta prohibición no afectará el derecho de los herederos de acceder a los contenidos que pudieran formar parte

del caudal relicto. Pero esto es muy impreciso, ya que no se indica expresamente qué debe incluirse; pareciera entenderse, que, si los contenidos no forman parte del caudal, la prohibición impediría acceder al contenido, en el caso de que la persona fallecida lo prohíba.

El tratamiento de los datos personales del fallecido por el sistema español no garantiza la intimidad-privacidad y otros derechos de la personalidad *post mortem*. Pero es más avanzado que los ya estudiados en este trabajo, pues regula expresamente el respeto a la voluntad del muerto. A pesar de que existe una atenuación de la voluntad del titular de los datos personales del fallecido ante los intereses sucesorios, la idea introducida en la legislación española servirá de inspiración para una propuesta de solución al problema central de esta investigación.

Otro Estado miembro de la Unión Europea que regula el tratamiento de datos de las personas fallecidas es Francia. La Ley 2016-1321, de 7 de octubre de 2016, actualizó el sistema legal francés de protección de datos personales para priorizar la voluntad del titular. Así, al modificar disposiciones de la Ley 78-17, de 6 de enero de 1978, la Ley 2016-1321, especialmente en el artículo 63, actualizó las reglas para el tratamiento de los datos personales del difunto, priorizando la voluntad del titular. Con la actualización, el artículo 40.1 de la ley enmendada ahora establece lo siguiente:

> [A]rtículo 40-1. I. Los derechos abiertos a esta sección expiran con la muerte de su titular. Sin embargo, pueden mantenerse provisionalmente de conformidad con los puntos II y III siguientes.
> II. Cualquier persona puede definir directrices con respecto al almacenamiento, eliminación y comunicación de sus datos personales después de su muerte. [...]
> III. En ausencia de directrices o de mención en contrario en las directrices antes mencionadas, los herederos del interesado podrán ejercer después de su muerte los derechos mencionados en esta sección, en la medida del necesario:
> -la organización y liquidación de los bienes del fallecido. Como tal, los herederos pueden acceder al tratamiento de los datos personales que les conciernen, con el fin de identificar y obtener la comunicación de información

> útil para la liquidación y división de activos. También pueden recibir comunicaciones de bienes digitales o datos que se asemejen a recuerdos familiares, que pueden ser transmitidos a los herederos;
> - la consideración, por parte de los responsables del tratamiento, de la muerte. Como tal, los herederos pueden cerrar las cuentas del usuario fallecido, oponerse a la continuación del tratamiento de los datos personales que le conciernen o proceder a su actualización.

A partir de esta modificación, cualquier persona puede ejercer los derechos de conservación, eliminación y la comunicación de sus datos posterior a su muerte en virtud de las denominadas instrucciones generales y específicas, las que a su vez pueden ser revocadas en cualquier momento. Las directrices generales están referidas a todos los datos personales relacionados con el sujeto, mientras que las específicas son objeto del consentimiento específico de la persona interesada y no pueden resultar de la aprobación exclusiva por parte de este último de las condiciones generales de uso de los servicios (Font; Boff, 2019, p. 41).

En el caso de Francia, se prefiere reconocerle prioridad a la voluntad del causante, que puede designar a la persona que él quiera para ejecutar sus instrucciones sobre la conservación, cancelación y comunicación de sus datos personales, una vez que haya fallecido. En la falta de designación, serán exclusivamente los herederos quienes podrán solicitar la ejecución de esas directrices. En defecto de instrucciones, esos mismos herederos estarán legitimados para ejercitar tales derechos, pero solo en la medida necesaria para la organización y regulación de la sucesión del difunto (Imbernón, 2020, p. 252).

En la misma dirección, Font y Boff (2019, p. 42) destacan que a falta de la designación de una persona responsable de la ejecución de las voluntades digitales o en caso de muerte de la persona designada, los herederos de la persona fallecida tendrán derecho al ejercicio de los derechos mencionados en la medida necesaria para la organización y liquidación de la sucesión.

De la comparación de los sistemas de España y Francia para la protección de los datos personales, en opinión de Imbernón (2020, pp. 253-254), parece preferible la solución por la que se ha decantado el legislador francés de hacer

primar la voluntad del causante a la hora de designar a la persona que puede ejercitar los derechos de acceso, rectificación o cancelación de sus datos personales una vez fallecido y, solo en defecto de designación, señalar a los herederos como segundo grupo de depositarios de esta confianza y al solo efecto de obtener la información necesaria para la partición de la herencia del causante o de defender su personalidad pretérita.

Tanto el sistema español como el francés garantizan al titular la posibilidad de crear directrices o prohibir el tratamiento de datos personales *post mortem*; si bien, la ley española, al limitar esta posibilidad a los datos personales que no tengan carácter patrimonial, brindando el acceso irrestricto a otros datos, no protege adecuadamente la intimidad y la privacidad del difunto.

Para una protección más adecuada de los derechos de la personalidad de los fallecidos es necesario un sistema más restrictivo, como el francés. La supremacía de la voluntad del titular de los datos personales es fundamental, incluso en relación a los datos personales con carácter patrimonial. Pero el punto más importante previsto en la legislación francesa es la limitación del acceso de los herederos cuando no existe manifestación expresa de la voluntad del fallecido. Se vio que, en este caso, el acceso sólo se autoriza en la medida necesaria para garantizar la satisfacción de los derechos sucesorios.

Es posible que el otorgamiento de acceso irrestricto a familiares pueda lesionar los intereses de terceros que, a través de los canales digitales, mantuvieron una relación con el fallecido, a través del desvelamiento de su vida privada. Asimismo, la falta de acceso a los herederos del fallecido también podría vulnerar intereses legítimos de estos titulares, dando lugar a la posibilidad de apropiación indebida por parte de las empresas propietarias de las plataformas que hacen posible los bienes digitales (Zampier, 2021, p. 256).

La restricción del derecho de acceso, en la forma del sistema francés de protección de datos personales, garantiza la protección mínima de los derechos de la personalidad *post mortem*, en la medida en que privilegia estos derechos en detrimento de los derechos meramente patrimoniales de los sucesores. Y así debe ser, porque en el conflicto entre los derechos de la personalidad y los derechos

sucesorios, éstos deben prevalecer porque involucran una mayor cantidad de derechos humanos fundamentales.

Se sabe que por abundante regulación que exista, realmente es una ardua tarea encontrar un modelo único que pueda satisfacer, al mismo tiempo, el derecho de acceso de la familia, los posibles deseos del fallecido, los intereses de terceros que mantuvieron contacto con él y también de los proveedores. No existe una estandarización expresa que resista a una gama tan amplia de intereses. Más de las veces, la ley se construye a partir de la conciliación y el sacrificio, que es una condición natural para la pacificación o acomodación social (Zampier, 2021, p. 257).

Spina y Giler (2019, p. 4) señalan, que “En caso de referirse a bienes digitales extrapatrimoniales relacionados con derechos personalísimos, se podría disponer de ellos mediante un testamento o de directivas anticipadas de autoprotección”. No obstante, las autoras citadas, afirman para el caso argentino, que “En tanto no haya legislación, la única protección que puede ofrecerse es la que surja de la preocupación del futuro causante que, en ejercicio de su autonomía de la voluntad, la prevea en un testamento o en un acto de autoprotección o directiva anticipada y entregue al notario en sobre cerrado, las cuentas y las claves de acceso, las que podrán irse renovando periódicamente” (p. 43). Sobre el vacío legal advertido, recomiendan aplicar lo dispuesto en el CCyCN (artículo 2379) a todo el universo digital de contenido personalísimo, hasta tanto no exista una normativa específica en la materia.

> […] Los objetos y documentos que tienen un valor de afección u honorífico son indivisibles, y se debe confiar su custodia al heredero que en cada caso las partes elijan y, a falta de acuerdo, al que designa el Juez. Igual solución corresponde cuando la cosa se adjudica a todos los herederos por partes iguales (artículo 2379).

Es en esta línea que se sugiere un cambio en los sistemas argentino y brasileño de protección de datos personales, para que se dicten leyes inspiradas, principalmente, en la normatividad de Francia. Pero, además, también se entiende que el sistema francés aún deja lagunas, ya que no explica cómo interpretar qué

es “acceso en la medida necesaria” para garantizar los derechos sucesorios, cuando no existen directivas del titular fallecido.

Más allá de lo expuesto, y teniendo presente el vació legal manifiesto, la sugerencia es que, en tales situaciones, se requiera de un análisis judicial de los límites de acceso, que serán otorgados a los sucesores. En esta línea, Fernández (2019, p. 64) aclara que, tradicionalmente, se ha sostenido que las medidas que importan una intromisión en la vida privada de las personas, como por ejemplo los allanamientos de sus hogares o la interceptación de su correspondencia o comunicaciones, requieren de la intervención y orden de un juez competente.

De esta forma, un juez sería la figura más adecuada para analizar y ponderar los derechos de los herederos y los derechos del fallecido, garantizando el respeto a la intimidad, a la privacidad y demás derechos de la personalidad del fallecido.

Capítulo VI: Marco Metodológico

Antes de la conclusión de esta tesis se presentan las siguientes consideraciones sobre la metodología empleada en la investigación y producción del trabajo. Aquí se debatió sobre temas relacionados con la intimidad, la privacidad y la protección de datos de personas fallecidas con el objetivo de identificar el alcance de la protección de la intimidad-privacidad *post mortem* garantizada por los sistemas argentino y brasileño de protección de estos activos digitales. Para ello, se analizaron documentos doctrinales y normativos nacionales y extranjeros, además de precedentes de los poderes judiciales de ambos países. La base de este trabajo también incluyó la investigación cuantitativa ya existente, relacionada con el tema.

En el proyecto original de este trabajo, el objetivo fue identificar el alcance de la protección de la privacidad de los fallecidos por los sistemas de protección de datos personales de Argentina y Brasil. No obstante, con el inicio de la investigación, se entendió que la intimidad *post-mortem* también podría ser el objetivo del estudio, sin desvirtuar el objetivo general inicial, dada su cercanía al instituto de privacidad. Así, el análisis realizado en esta tesis consideró la protección de estos dos derechos fundamentales de acuerdo con las normas de protección de datos personales de los dos países.

Para alcanzar el objetivo general, se delinearon seis objetivos específicos, a saber: (1) comparar las normas jurídicas y las jurisprudencias de Argentina y Brasil acerca de la protección de datos; (2) señalar qué alcance reviste el derecho a la intimidad-privacidad en Argentina y Brasil respecto a los datos e informaciones privadas de las personas vivas guardadas en Internet; (3) identificar las políticas de registro y almacenamiento de datos de las redes sociales más utilizadas en Argentina y Brasil; (4) dar cuenta de la utilidad de los datos de personas fallecidas que vagan por internet; (5) identificar el tratamiento jurídico dado por la España respecto a los datos e informaciones íntimas y/o privadas de las personas fallecidas guardadas en Internet; y (6) realizar una propuesta jurídica que

contemple como salvaguardar la utilización de los datos de las personas fallecidas guardados en Internet en Argentina y Brasil.

Dichos objetivos fueron considerados durante el desarrollo de los capítulos de este trabajo. El Capítulo II presentó los resultados del objetivo específico 1, que expuso las normas que conforman los sistemas de protección de datos personales en Argentina y Brasil y el comportamiento de sus tribunales superiores. Este objetivo se logró a través de la consulta de documentos normativos –leyes, constituciones y proyectos de ley– y decisiones judiciales encontradas en búsquedas específicas realizadas en los sitios *web* de los tribunales superiores de ambos países.

En cuanto a las normas jurídicas, los resultados mostraron que Argentina y Brasil cuentan con sistemas jurídicos robustos y complejos para la protección de datos personales conformados principalmente por disposiciones legales y constitucionales; si bien se encuentran en diferentes momentos en la evolución y actualización de estos sistemas.

Sobre la jurisprudencia, se evidenció que los tribunales superiores de las dos naciones no han tratado el tema, lo que refleja una baja judicialización de demandas en materia de protección de datos personales. Por ello, los escasos datos jurisprudenciales encontrados dificultaron la comparación inicialmente propuesta, pero demostraron que los tribunales consultados han abordado de manera similar el tema en un contexto más amplio, generalmente involucrando también otros derechos como la imagen, la moral y el honor.

Los objetivos específicos 2 y 3 se consolidaron en el Capítulo III. Para señalar, de acuerdo con el objetivo 2, la protección jurídica de la privacidad e intimidad de las personas vivas garantizada por los sistemas argentino y brasileño de protección de datos personales, inicialmente se desarrolló un análisis de valoración de los datos de personas vivas, identificando cuáles es el valor y quiénes están interesados en este tipo de material. También se señaló la importancia del consentimiento en el tratamiento de datos personales, demostrando la evolución y la esencialidad –actualmente mitigada– de este instituto.

La satisfacción del objetivo específico 2 se dio a través del uso de datos cuantitativos y cualitativos provenientes de investigaciones existentes sobre la percepción de la importancia y valor de los datos personales, doctrina especializada y mecanismos para la cuantificación de datos personales, como es el caso de calculadora de datos presentada en el capítulo respectivo.

Para cumplir con el objetivo específico 3 se identificaron las redes sociales más utilizadas en Brasil y Argentina y se analizaron sus políticas de datos, mostrando comportamientos diferentes para cada una. El resultado encontrado en este objetivo ayudó en la propuesta de una solución legal para el problema central del trabajo. Este objetivo específico se logró mediante el análisis documental de las políticas de privacidad puestas a disposición en Internet por las redes sociales, las cuales fueron elegidas de acuerdo a los datos presentados en el informe Digital en 2020, de las consultorías *We Are Social* y *Hootsuite*.

El capítulo IV incluye la contemplación del objetivo específico 4 que proporciona información sobre la utilidad de los datos de personas fallecidas que circulan por Internet, señalando cómo se ha utilizado este material en la sociedad de la información. La consecución del objetivo en foco también señaló los riesgos que corre la intimidad-privacidad *post-mortem* con el tratamiento de este tipo de datos.

Así, luego de un análisis del “Derecho al Olvido”, se sugirió el uso de este instituto con una guía para la protección de la intimidad y la privacidad *post mortem*. Para lograr el objetivo en foco se utilizaron noticias periodísticas que demuestran cómo las empresas han utilizado los datos personales del fallecido, además de datos normativos nacionales y extranjeros y doctrina especializada.

Los resultados de los objetivos específicos 5 y 6 se presentan en el capítulo V. Aquí, en un principio, se buscó identificar el tratamiento legal que da España a los datos e información privada de personas fallecidas almacenados en Internet. Igualmente, el cumplimiento de este objetivo demostró que la legislación española no reflejaba un tratamiento adecuado sobre el tema. Por lo tanto, el objetivo fue extrapolado, ampliando la investigación a la legislación francesa, lo que resultó en una mejor promoción del próximo objetivo específico. Para alcanzar el objetivo

específico 5 se utilizaron documentos normativos europeos, españoles y franceses, además de doctrina especializada.

El último objetivo específico trajo una propuesta de solución al problema central de este trabajo a partir de los resultados obtenidos al contemplar los objetivos anteriores, en particular, los objetivos 3 y 5. En otras palabras, se utilizaron los resultados de la investigación que involucró a las redes sociales y los derechos de España y Francia para sugerir cómo Argentina y Brasil pueden actuar para salvaguardar los datos de personas fallecidas almacenados en Internet. Con ello, el trabajo alcanzó la satisfacción del objetivo general, que confirmó parcialmente la hipótesis inicial, la que será ampliada en el próximo Capítulo.

En efecto, esta tesis se estructuró en la introducción mediante la matriz conformada por seis capítulos de desarrollo, su conclusión, la bibliografía y las fuentes pertinentes de la información aportada al presente trabajo de doctorado. Dentro del desarrollo, cada capítulo contempló uno o dos objetivos específicos. El objetivo general se alcanzó al final, en la conclusión. Esta estructura fue elegida para cumplir mejor cada objetivo del trabajo, considerando la afinidad e individualidad de cada uno de ellos.

En cuanto a la hipótesis presentada, es una hipótesis de constatación. Siguiendo a Dieterich (1999, p. 119) una hipótesis de constatación es una proposición científica –un enunciado– que, con fundamento en el conocimiento científico trata de constatar la presencia o ausencia de un fenómeno o de una propiedad de un fenómeno.

En el caso de esta investigación, la hipótesis encontró que en Argentina y Brasil no existe una adecuada protección legal de la intimidad y privacidad *post mortem* a través de los respectivos sistemas jurídicos de protección de datos personales. Así, el establecimiento de la ausencia del fenómeno de tutela jurídica de los institutos antes mencionados justifica enmarcar la hipótesis como una hipótesis de constatación.

Debe considerarse, entonces, que este trabajo se originó a partir de una investigación *lege lata*. Como enseña Queiroz (2011, p. 21), este tipo de investigación opta por un problema interpretativo-jurídico como objeto y busca

aclararlo y ofrecer la respuesta que considera la mejor respuesta jurídica, considerando las disposiciones legales vigentes en la materia en cuestión.

La metodología utilizada en este trabajo fue no experimental y utilizó la investigación documental y jurisprudencial, y la estrategia de análisis de contenido. En efecto, las unidades de análisis fueron documentos normativos sobre protección de datos personales, intimidad y privacidad, nacionales y extranjeros, doctrina nacional e internacional, y la jurisprudencia de Argentina y Brasil, relacionada con el tema central, además de la investigación cuantitativa existente. Por estos factores la investigación también se considera cualitativa.

En este caso debe observarse, que la investigación cualitativa abandona el ámbito puramente académico, despertando el interés de quienes piensan y desarrollan políticas públicas, de quienes buscan investigaciones orientadas al estudio de problemas sociales e instituciones orientadas a la búsqueda de sus soluciones.

El trabajo también tuvo como principales variables la vulnerabilidad de la intimidad y privacidad *post mortem* y el alcance de la protección de los datos personales existentes. En este paso, el marco temporal fue la fecha de publicación de la Ley General de Protección de Datos de Brasil, que tuvo lugar el 14 de agosto de 2018.

No obstante, en vista de la existencia relativamente reciente de esta legislación y la consecuente escasez de doctrina relacionada con el problema que se resolvió con la investigación, fue necesario consultar el marco teórico, normativo y jurisprudencial anterior, con el objetivo de lograr una profunda inmersión en el campo de estudio en la búsqueda de soluciones que aún no existen.

En cuanto a los datos jurisprudenciales, se utilizaron parámetros similares para la búsqueda de sentencias en los tribunales de Argentina y Brasil. El período relevado abarcó el tiempo comprendido entre el 14 de agosto de 2018 (fecha de publicación de la Ley General de Protección de Datos Personales en Brasil) y el 8 de diciembre de 2019 (fecha de consulta).

Los términos utilizados en la búsqueda realizada en el sitio *web* de la Corte Suprema de Brasil fueron las expresiones “Privacidade e Proteção de Dados Pessoais”, “Lei Geral de Proteção de Dados Pessoais” y “Lei 13.709/2018”. Sin embargo, no hubo sentencia de la Corte Suprema, sino solo tres fallos, ninguno de los cuales tiene una relación directa con la violación de la privacidad y la protección de datos personales.

En las búsquedas realizadas en los sitios *web* de la Corte Suprema de Justicia de la Nación Argentina, de la Cámara Nacional de Apelaciones en lo Civil y de la Cámara Nacional de Apelaciones en lo Civil y Comercial Federal, se usó la expresión “Privacidad y Protección de Datos Personales”, obteniendo un resultado idéntico de ausencia de sentencias.

El único tribunal que presentó resultados fue el Superior Tribunal de Justicia de Brasil. En la consulta realizada al acervo de jurisprudencia de esta Corte, repitiendo los parámetros de la investigación realizada en la Corte Suprema del país, surgieron algunas decisiones que aportaron a la consolidación del resultado de este trabajo.

El corte temático ayudó a adecuar la investigación jurisprudencial a la delimitación del tema. Palma, Feferbaum y Pinheiro (2014, p. 145) explican que, a través del corte temático, el investigador elige un tema específico entre varios posibles para ser objeto de análisis en su trabajo. Tal corte se caracterizó en las investigaciones realizadas en los fondos jurisprudenciales disponibles en los sitios *web* de los tribunales mencionados.

El marco temporal que, según Palma, Feferbaum y Pinheiro (2014, p. 145) corresponde al período en el que se analizan las decisiones, se consideró libre, ya que, en el marco temporal iniciado con la entrada en vigor de la Ley General de Protección de datos brasileños, no se encontraron resultados importantes. Por tanto, en cuanto al tiempo, se entiende que la investigación es longitudinal.

Mediante la observación indirecta de documentos normativos y jurisprudenciales, y de la doctrina relacionada se dominó el tema y se identificaron las soluciones actuales y futuras al problema. Respecto a la solución actual, se sugirió la aplicación del “Derecho al Olvido” a los datos personales de los

fallecidos, mientras no exista una adecuada protección legal de estos activos digitales. En cuanto a la solución futura, se señaló la posibilidad de sancionar leyes en Argentina y Brasil que llenen el vacío normativo existente sobre el tema.

Según Mezzaroba (2017, p. 90) el método inductivo nos permite analizar nuestro objeto para sacar conclusiones generales o universales. Así, a partir, por ejemplo, de la observación de uno o algunos fenómenos particulares, se establece una proposición más general para, a su vez, ser aplicada a otros fenómenos. Es, por tanto, un procedimiento generalizador.

Finalmente, la investigación también tuvo un carácter interdisciplinario, ya que se buscó la interacción entre Derecho y Tecnología. Sobre esta especie, Leister y Wang (2014) opinan que “el valor de la investigación interdisciplinaria [...] se siente poco en la academia, habiendo sido más percibido por el mercado” (p. 193).

Lo expuesto abre una fundada expectativa en el autor de esta tesis de doctorado, que es la de poder ofrecer un aporte a la labor de los estudiosos y operadores del Derecho y la Tecnología, hasta tanto el tema sometido a estudio no gane más espacio en los ámbitos legislativo, doctrinal y judicial de la Argentina y Brasil. Asimismo, se espera que este trabajo pueda ayudar a futuras investigaciones sobre datos personales e informaciones privadas de las personas fallecidas, en la búsqueda de soluciones legales destinadas a salvaguardar el derecho a la intimidad-privacidad y otros derechos de la personalidad *post mortem*.

Conclusión

Son diversas las denominaciones empleadas para categorizar al actual momento de disrupción por el que atraviesa el mundo. Revolución tecnológica, revolución digital, revolución tecnológica digital o cuarta revolución industrial, por citar ejemplos, incluyen la voz revolución. Es esta palabra la que mejor define la realidad de diversos conceptos históricamente consolidados, y que actualmente navegan por un océano de marcada incertidumbre jurídica. Algunos de estos conceptos -vida, muerte, intimidad y privacidad- fueron abordados en este trabajo, y en cada uno de ellos se pudo observar que atraviesan por una etapa de inestabilidad, producto de su tránsito al universo virtual.

Los conflictos entre esos conceptos y la necesaria, casi obligatoria, inserción de la tecnología en la vida cotidiana generan problemas como lo que motivó la elaboración de esta tesis. La intimidad y privacidad después de la muerte están en el centro de la investigación que se lleva a cabo, porque si en el caso de la persona viva ya es muy difícil de proteger este derecho de la personalidad, en el caso del fallecido la complejidad se vuelve aún mayor. Las personas vivas tienen a su disposición numerosas herramientas legales y tecnológicas para intentar salvaguardar su intimidad-privacidad; en cambio, las fallecidas se encuentran, de por sí, indefensas.

El principal factor de riesgo para la intimidad y privacidad en la sociedad de la información son los datos personales, que la ley define como información relacionada con la persona humana identificada o identificable. Son ellos quienes llevan la información de todas las acciones de cada individuo, incluidas las de carácter íntimo, y por tiempo indefinido. No hay fecha de vencimiento para los datos personales. Existirán para siempre si no se suprimen.

Aquí es donde radica la preocupación planteada en la problemática de este trabajo, que buscó entender si los sistemas de protección de datos personales en Argentina y Brasil son capaces de garantizar el tratamiento de estos activos digitales sin violar la intimidad-privacidad de una persona fallecida. La respuesta ya se ha dado en los capítulos anteriores y se consolidará más adelante.

Argentina y Brasil atraviesan realidades diferentes en cuanto a la protección legal de los datos personales. La Nación argentina, que ya ha sido una referencia en América Latina por ser pionera en la materia, atraviesa actualmente una larga e injustificada espera para actualizar su ordenamiento jurídico de protección de datos personales, que aún tiene como regla principal una ley sancionada a comienzos del siglo XX.

A medida que avanza la tecnología y el uso de medios tecnológicos, a una velocidad que se intensificó aún más con la pandemia Covid-19, el país deja a sus ciudadanos a merced de una estandarización anticuada. Hace más de dos décadas que rige una ley de datos personales, que ha quedado obsoleta y deja al país atrás, frente a otras naciones que han estado tratando de adaptarse al escenario internacional.

Por el contrario, desde 2018, Brasil cuenta con una ley de protección de datos personales profundamente inspirada en la normativa de la Unión Europea, lo que coloca al país en el camino de la adaptación internacional en la materia. La gran polémica es la demora en la entrada en vigencia de todo el texto de la norma, que solo ocurrirá en el 2021.

Anteriormente (2014), el país ya había hecho grandes avances en la estandarización de la protección de datos personales, con la edición de una ley que se conoció como el Marco Civil de Internet. Esta ley inició las negociaciones para la emisión de una ley general de protección de datos personales, lo que sucedió cuatro años después.

En esta distinción de realidades, se encontró que otras normas tratan la protección de datos personales en ambos países, conformando así sistemas jurídicos que garantizan, en la actualidad, un mínimo de seguridad para sus ciudadanos. Se tratan de normas relacionadas con las relaciones con el consumidor, la propiedad intelectual y la información pública, por ejemplo, que obviamente tratan otros temas, pero que terminan llevando su tutela al ámbito de la protección de los datos personales, de la intimidad y privacidad.

En ausencia de leyes más completas, el poder judicial tiene la tarea de garantizar la protección adecuada de los datos y los derechos de la personalidad

en la sociedad de la información. Pero en la búsqueda realizada en este trabajo en los tribunales superiores de Argentina y Brasil, lo que se encontró fue una escasez de sentencias al respecto, lo que demostró que aún no existe una jurisprudencia formada capaz de suplir satisfactoriamente el carácter incompleto de las protecciones legales existentes en ambos países.

Habitualmente, ante la ausencia de reglas específicas para problemas sociales recurrentes, el Poder Judicial asume el protagonismo de las situaciones, lo que no ocurre en la protección de datos personales. Luego, la velocidad con la que surgen los problemas relacionados con la tecnología no es compatible con la lentitud del poder judicial.

El Estado se ha mostrado incapaz de resolver, con la rapidez necesaria, situaciones como la señalada en el problema central de esta tesis. Y para empeorar las cosas, los datos personales comenzaron a adquirir una importancia económica considerable, requiriéndose con mayor urgencia, la protección legal por parte del Estado. El tema de los datos personales ya no se limita un solo ámbito del derecho, ya que se comunican con los diferentes ámbitos del derecho público y privado. Están presentes en prácticamente todo, desde las relaciones privadas hasta las relaciones internacionales entre Estados.

Los datos personales se convierten en activos económicos, asumiendo las características de los bienes digitales, que se comercializan y se transforman en objetos de sucesión hereditaria. Lee (2019, p. 270) ya dijo que nuestros gobiernos deberán examinarse unos a otros cuando evalúen nuevas y delicadas compensaciones en términos de privacidad de datos, monopolios digitales, seguridad en línea y tendencias algorítmicas.

La doctrina intenta separar los datos que tienen valor económico de los que no tienen importancia patrimonial, en un intento por crear una adecuada protección jurídica, tarea que no ha sido fácil.

En relación a los datos personales de importancia económica, hubo una enorme dificultad de cuantificar el valor real, concluyendo sólo que, para el mercado, la información aislada de un individuo común no tiene ninguna relevancia. El foco de las empresas que están interesadas en estos activos

digitales se gira a grandes cantidades de datos, ya que es este conjunto que realmente garantiza una mayor eficacia de las acciones de mercado.

Respecto de los datos personales sin carácter patrimonial, las complicaciones son aún mayores. Estos bienes digitales acaban siendo menos observados por los legisladores, que simplemente, en la mayoría de los casos, no regulan la temática. Olvidan, que más de las veces, este tipo de datos personales llevan información que no le interesa al titular para publicarlos, lo cual está garantizado por la inviolabilidad de su intimidad-privacidad, derecho que tiene jerarquía constitucional en la mayoría de países democráticos. No es que los legisladores ignoren este hecho, porque, aparentemente, le dieron al interesado el deber de proteger su intimidad y privacidad a través de la forma del consentimiento.

Por lo tanto, el consentimiento ha sido el mecanismo más importante para proteger los datos personales en la realidad actual de la sociedad de la información. La legislación en todo el mundo ha reforzado la necesidad de que la manifestación de la voluntad encarnada en el consentimiento se descarte de cualquier adicción, omisión, oscuridad o desinformación.

Pero la evolución de las leyes de protección de datos ha creado otras figuras que permiten el acceso a los datos personales, tomando parte del protagonismo en la materia desde el consentimiento. Por caso, aquellos datos que no tienen importancia patrimonial, cuando se caracterizan datos sensibles, los desarrollos legislativos mantuvieron la regla de otorgar el consentimiento para el acceso a este tipo de información.

La protección particular de los datos personales a través del instituto del consentimiento puede ser una de las causas de la no normatividad de las cuestiones relacionadas con la intimidad y privacidad en la era de la revolución tecnológica. Es este tipo de protección la que prima, por ejemplo, en las relaciones entre las redes sociales, cada vez más presentes y necesarias en las relaciones humanas, y los titulares de los datos personales. Además de la escasa estandarización, el carácter transnacional de estos mecanismos de interacciones

sociales refuerza la importancia de la protección privada de los datos personales a través del consentimiento.

También es debido a este carácter transnacional que las redes sociales crean sus propios sistemas normativos para procesar los datos personales de los usuarios. Así se verificó en el análisis realizado en las políticas de privacidad y almacenamiento de datos de las redes sociales más utilizadas en Argentina y Brasil.

YouTube, *WhatsApp*, *Facebook* e *Instagram* fueron el tema de este estudio, donde se identificó que cada una de estas redes sociales tiene sus propias reglas para manejar los datos personales y garantizar la intimidad y privacidad. Todos ellos centrados en el consentimiento sus formas de iniciar, realizar y dar por terminado el tratamiento de los datos del usuario, lo que refuerza la idea de la efectividad de la tutela privada.

Pero cuando se trata de proteger los datos personales de un fallecido, cada una de las redes sociales analizadas se comporta de manera diferente. Mientras *YouTube/Google* dejan a su criterio la posibilidad de acceder a los datos del usuario fallecido, *WhatsApp* se compromete a eliminar, unilateralmente, los datos.

Facebook e *Instagram*, por su parte, aseguran que en ningún caso darán acceso a los datos personales que formen parte del contenido de las cuentas, permitiendo únicamente la solicitud por parte de terceros de borrar las cuentas o, incluso, su transformación en memoriales administrados por un sucesor (posibilidad exclusiva de *Facebook*) o por las propias redes sociales. Así, a excepción de la postura de *YouTube/Google*, las medidas tomadas por otras redes sociales garantizan la intimidad-privacidad *post mortem* del usuario, ya que no permiten el acceso de terceros a los datos de contenido de la cuenta.

Al parecer, los datos de una persona fallecida son de poca utilidad; afirmación que pierde fuerza en la sociedad de la información. En primer lugar, porque parte de este tipo de datos adquirió un carácter patrimonial y, en segundo lugar, porque eternizan la información sobre alguien que ha fallecido, si no se excluye.

Luego se demostró que los datos de los fallecidos, incluidos los que no tienen características patrimoniales, exigen protección legal. Ya no es posible ignorar que los datos personales se han convertido en bienes digitales y se utilizan, incluso aquellos que no tienen valor económico, para los más variados fines.

Los datos personales de un fallecido son objeto de los más variados intereses y la limitación del consentimiento ya no puede utilizarse en el tratamiento. Se asemejan a explosivos reales que pueden detonar la intimidad, la privacidad y otros derechos de la personalidad después de la muerte. Es por ello que la necesidad de normatizar el tratamiento de los datos personales de los fallecidos, especialmente de aquellos que puedan exponer indebidamente los derechos de la personalidad, es algo tan presente, como urgente.

Fue con esta preocupación que se desarrolló este trabajo para comprender en qué medida los sistemas jurídicos de protección de datos personales en Argentina y Brasil garantizan la intimidad-privacidad de las personas después del fallecimiento. Volviendo a la hipótesis inicial, donde se consideró que los dos países no protegerían adecuadamente, a través de dichos sistemas, la intimidad y privacidad *post mortem*, la conclusión es que se confirmó.

De hecho, los sistemas argentino y brasileño de protección legal de datos personales no protegen adecuadamente este tipo de derecho de personalidad. En el caso de Argentina, la norma transmite el acceso a los datos del fallecido a los sucesores sin limitar el ejercicio de este derecho. En el caso de Brasil, la legislación no contiene disposiciones expresas, siendo el principio de finalidad, una de las balizas favorables a los muertos.

La confirmación de la hipótesis es porque no se puede ignorar que existen normas legales en los dos países, ligadas o no a los avances tecnológicos, que protegen mínimamente la intimidad y privacidad del fallecido, incluso cuando se relacionan con el tratamiento de datos personales. Pero son reglas escasas y/o genéricas que exigen un cierto esfuerzo del operador del derecho, generando decisiones controvertidas. Así, más allá de que existen normas en ambos países la protección es insuficiente.

Por ello, se señaló, como una guía para el adecuado tratamiento de los datos personales del difunto, que tienen el potencial de dañar la intimidad-privacidad, la aplicación del “Derecho al Olvido”, hasta que surjan normas que garanticen la efectividad en la protección de los derechos de la personalidad *post mortem*.

La experiencia de uso de este derecho ya se puede ver en las políticas de redes sociales analizadas en este trabajo, principalmente *WhatsApp*, *Facebook* e *Instagram*. De manera indirecta, estas redes sociales garantizan la intimidad y privacidad de los usuarios fallecidos al denegar el acceso a los contenidos de las cuentas, lo que se traducirá en el olvido de los datos respectivos.

Y, como una forma de resolver el problema central presentado en esta tesis, se sugirió la sanción de leyes en Argentina y Brasil inspiradas en los marcos regulatorios de España y Francia, que garanticen al titular la posibilidad de dejar una prohibición o directrices para el tratamiento de sus datos personales, posteriores a la muerte. La sugerencia fue de mayor inspiración en el sistema francés, que prioriza la voluntad de los fallecidos en detrimento de los derechos de los sucesores; situación que no se da en el sistema español.

El rigor del sistema en Francia garantiza una mayor seguridad a los derechos personales del fallecido, ya que el permiso de acceso por parte de los sucesores solo será en la medida necesaria para la satisfacción de los derechos sucesorios. Finalmente, para reforzar esta restricción, se sugirió que el análisis de la “medida necesaria” sea realizado por un órgano judicial, que garantice el justo equilibrio entre los derechos de los herederos y el fallecido.

Con ello, se espera, que el presente trabajo contribuya para la consolidación de los sistemas de protección de datos personales más robustos en Argentina y Brasil, y ayude a académicos y operadores legales en la elaboración de soluciones a los vacíos regulatorios existentes. También se anhela, que sirva de base para futuros estudios sobre protección de datos e intimidad-privacidad *post mortem* en la sociedad de la información, además de servir como material de apoyo para las decisiones de mercado y para las personas que utilizan los diversos medios masivos de comunicación, en constante expansión y evolución tecnológica.

Bibliografía y fuentes de información

Bibliografía

Addati, F. A. (2020). El impacto de las redes sociales en los derechos personalísimos. *Ratio Iuris*, 35-81. Recuperado de http://dspace.uces.edu.ar:8180/xmlui/bitstream/handle/123456789/5399/El%20impacto_Addati.pdf?sequence=1

Almeida, B. A., Doneda, D., Ichihara, M. Y., Barral-Netto, M., Matta, G. C., Rabello, E. T., y Barreto, M. (2020). *Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global* [Preservación de la privacidad en la lucha contra COVID-19: datos personales y pandemia global]. *Ciência & Saúde* Coletiva [online], *25*(1), 2487-2492. doi: 10.1590/1413-81232020256.1.11792020.

Amendola, D., y Carneiro, C. D. R (2019). *Análise crítica de conceitos de geologia apresentados na plataforma Youtube® com foco em vídeo-aulas* [Análisis crítica de los conceptos de geología presentados en la plataforma Youtube® con un enfoque en lecciones en video]. *Terrae Didatica*, *15*, 1-9. doi: 10.20396/td.v15i0.8657523

Andréa, G. F. M., Arquite, H. R. L., y Camargo, J. M. (2020). Proteção dos dados pessoais como direito fundamental: a evolução da tecnologia da informação e a Lei Geral de Proteção de Dados no Brasil. [Protección de datos personales como derecho fundamental: la evolución de la tecnología de la información y la Ley General de Protección de Datos de Brasil]. *Thomson Reuters Legal One, 1-20.* Recuperado de https://www.thomsonreuters.com.br/content/dam/openweb/documents/pdf/Brazil/revistas-especializadas/rdci-121-gianfranco-andrea-e-outros.pdf

Aneja, S., y Shapiro, R. (2019). *Who owns americans' personal information and what is it worth?* [¿Quién posee la información personal de los estadounidenses y cuál es su valor?]. *Future Majority, 1-22.* Recuperado de https://assets.futuremajority.org/uploads/report-for-future-majority-on-the-value-of-people-s-personal-data-shapiro-aneja-march-8-2019.pdf

Aragão, F. A. A., y Benevides, P. S (2019). *Governamentalidade algorítmica e Big data: o uso da correlação de dados como critério de tomada de decisão* [Gubernamentalidad algorítmica y Big Data: el uso de la correlación de datos como criterio para la toma de decisiones]. En *VI Simpósio Internacional Lavits*. Salvador, Bahia.

Arocena, G. A. (2012). La regulación de los delitos informáticos en el Código Penal argentino: introducción a la Ley Nacional núm. 26.388. *Boletín mexicano de derecho comparado*, *45*(135), 945-988. Recuperado de http://www.scielo.org.mx/pdf/bmdc/v45n135/v45n135a2.pdf.

Assunção, R. S., y Matos, P. M. (2014). *Perspetivas dos adolescentes sobre o uso do Facebook: um estudo qualitativo* [Perspectivas de los adolescentes sobre el uso de Facebook: un estudio cualitativo]. *Psicologia em Estudo*, *19*(3), 539-547. doi: 10.1590/1413-73722133716

Barreto, A. G., y Nery Neto, J. A. (2016). *Herança digital* [Herencia digital]. *Revista Eletrônica Direito & TI, 1*(5), 1-10*.* Recuperado de https://direitoeti.emnuvens.com.br/direitoeti/article/view/59

Barros, B. M. C., y Flain, V. S. (2016). *O marco civil da internet: um olhar sobre a proteção dos direitos e garantias dos usuários na sociedade em rede* [El marco civil de Internet: una mirada a la protección de los derechos y

garantías de los usuarios en la sociedad red]. En *IX Mostra Internacional de Trabalhos Científicos – UNISC.* (pp. 1-20). Santa Cruz do Sul.

Becerra, M. C., y Zárate, P. D. (2015). Intimidad y privacidad en entornos digitales luego de la reforma del Código Civil. En *15º Simposio Argentino de Informática y Derecho*. (pp. 216-226). San Juan, Argentina.

Becerra, M., y Garziglia, L. (11 de abril de 2019). Datos personales: hacia una nueva ley con viejas mañas [Publicación de Letra P]. Recuperado de https://www.letrap.com.ar/nota/2019-4-11-9-59-0-datos-personales-hacia-una-nueva-ley-con-viejas-manas

Beltrão, S. R. (2015). *Tutela jurídica da personalidade humana após a morte: conflitos em face da legitimidade ativa* [Tutela jurídica de la personalidad humana después de la muerte: conflictos ante la legitimidad activa]. *Revista de Processo, 247*, 1-13. Recuperado de http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/RPro_n.247.07.PDF

Benitez, A. C., Cabrera, N., y Ruidiaz, M. F (2019). Mochileros.net. *Actas de Periodismo y Comunicación*, *5*(2), 1-14. Recuperado de https://perio.unlp.edu.ar/ojs/index.php/actas/article/view/5855/5060.

Benjamin, A. H. V. y otros (2005). *Código brasileiro de defesa do consumidor comentado pelos autores do anteprojeto* [Código brasileño de protección al consumidor comentado por los autores del anteproyecto] (8a ed.). Río de Janeiro: Forense Universitária.

Bennett, C. (1992). *Regulating privacy: data protection and public policy in Europe and the United States* [Regulación de la privacidad: protección de datos y políticas públicas en Europa y Estados Unidos]. Ithaca, New York: Cornell University Press.

Beppu, F., y Maciel, C. (2020). *Perspectivas normativas para o legado digital pós-morte face à lei geral de proteção de dados pessoais* [Perspectivas normativas para el legado digital post-mortem bajo la ley general de protección de datos personales]. *Anais do I Workshop sobre as implicações da computação na sociedade* (pp. 73-84). Porto Alegre: SBC.

Bertoni, E. (2014). The Right to Be Forgotten: An Insult to Latin American History. [El derecho al olvido: un insulto a la historia latinoamericana.] [Publicación de Huffpost].Recuperado de https://www.huffpost.com/entry/the-right-to-be-forgotten_b_5870664

Bertoni, E. y Cortés Castillo, C. (2014). Derecho al olvido: entre la protección de datos, la memoria y la vida *personal en la era digital*. Internet y derechos humanos: aportes para la discusión en América Latina, 123-148. Compilado por Eduardo Andrés Bertoni. -1a ed.- Buenos Aires: Del Puerto.

Bidart Campos, G. J. (1995). *Tratado elemental de Derecho Constitucional*. Buenos Aires: Ediar.

Bidart Campos, G. J. (2014). *Manual de la Constitución reformada* (Tomo I). Buenos Aires: Ediar.

Bioni, B. R. (2019). *Proteção de dados pessoais: a função e os limites do consentimento* [Protección de datos personales: la función y los límites del consentimiento]. Río de Janeiro: Forense.

Bosque L., y Villan, M. A. (2018). Datos personales, marketing digital y los derechos de los ciudadanos de américa latina: estado de protección de los datos de los ciudadanos. En *VI Congreso Internacional de Ciencias Sociales*. Cancún, México. Recuperado de https://www.researchgate.net/publication/334576727_Datos_personales_marketing_digital_y_los_derechos_de_los_ciudadanos_de_America_Latina

Bottrel, R. M. (2018). *A contribuição do acesso à informação pública para a comunicação pública no Brasil* [La contribución del acceso a la información pública para la comunicación pública en Brasil]. *Comunicação Pública, 13* (24). doi:10.4000/cp.2234

Cadman, E., Freese, B., Locke, C., y Ssteel, E. (12 de junio de 2013). *How much is your personal data worth?* [¿Cuánto valen sus datos personales?]. [Publicación de Financial Times]. Recuperado de https://ig.ft.com/how-much-is-your-personal-data-worth/.

Calais, B. (10 de septiembre de 2020). *“Black Mirror” da vida real: brasileiro funda startup para recriar pessoas mortas* ["Black Mirror" de la vida real: brasileño funda startup para recrear muertos]. [Publicación de Forbes]. Recuperado de https://forbes.com.br/principal/2020/09/black-mirror-da-vida-real-brasileiro-funda-startup-para-recriar-pessoas-mortas/

Cánepa, I. C. (2019). Acerca de la incorporación de los derechos y actos peronsalísimos en el Código Civil y Comercial de la Nación. *Perspectivas de las Ciencias Económicas y Jurídicas*, *5*(1), 35-50. Recuperado de: https://cerac.unlpam.edu.ar/index.php/perspectivas/article/view/3636/3748

Cejudo, D. (11 de enero de 2020) ¿Cuánto valen nuestros datos personales? [Mensaje de Blog]. Recuperado de

https://www.diariodesevilla.es/sociedad/datos-personales-internet-valen_0_1426657625.html

Cerda Silva, A. (2012). Protección de datos personales y prestación de servicios en línea en América Latina. *Hacia una internet libre de censura: propuestas para América Latina*, 165-180. Compilado por Eduardo Andrés Bertoni. -1a ed.- Buenos Aires: Universidad de Palermo - UP. Recuperado de http://repositorio.uchile.cl/bitstream/handle/2250/139601/Proteccio%cc%81n_de_Datos_Personales.pdf?sequence=1&isAllowed=y

Cobiella, M. E. C. (2013). Protección post mortem de los derechos de la personalidad. Reflexionando sobre la cuestión. *Revista Boliviana de Derecho,15*, 112-129. Recuperado de http://www.scielo.org.bo/pdf/rbd/n15/n15a07.pdf

Costa, D. C. (10 de junio de 2019). *Transformando desafios em oportunidades: porque a LGPD e sua empresa podem ser a combinação perfeita* [Convertiendo desafíos en oportunidades: por qué LGPD y su empresa pueden ser la combinación perfecta]. [Mensaje de Blog]. Recuperado de https://migalhas.uol.com.br/depeso/304059/transformando-desafios-em-oportunidades--porque-a-lgpd-e-sua-empresa-podem-ser-a-combinacao-perfeita

Creste, M. V. A., y Tebar, W. B. C. (2017). A tutela do direito à intimidade e à privacidade perante o avanço das redes sociais [La tutela del derecho a la intimidad y la privacidad ante el avance de las redes sociales]. En *Encontro de Iniciação Científica.* (pp. 1-17). Presidente Prudente.

Dieterich, H. (1999). Nueva guía para la investigación científica (séptima reimpresión). Colonia del Valle: Ariel. Recuperado de

http://ual.dyndns.org/biblioteca/Seminario_de_tesis/pdf/Nueva_guia_investigacion_cientifica.pdf

Diniz, M. H. (2017). *Uma visão constitucional e civil do novo paradigma da privacidade: o direito a ser esquecido* [Una visión constitucional y civil del nuevo paradigma de la privacidad: el derecho al olvido]. *Revista Brasileira de Direito, 13*(2), 7-25. doi: 10.18256/2238-0604/revistadedireito.v13n2p7-25

Domínguez, E. R (2016). *La protección legal de los datos personales y el spam en el derecho argentino* (Tesis de Doctorado). Recuperado de https://repositorio.uesiglo21.edu.ar/bitstream/handle/ues21/10528/Entrega_Final2.doc?sequence=1

Dorado, J. G. (30 de mayo de 2016). Derecho a la intimidad y protección de datos personales en las condiciones de uso y políticas de privacidad de las redes sociales [Publicación de SAIJ]. Recuperado de http://www.saij.gob.ar/john-grover-dorado-derecho-intimidad-proteccion-datos-personales-condiciones-uso-politicas-privacidad-redes-sociales-dacf160315-2016-05-30/123456789-0abc-defg5130-61fcanirtcod?q=%28id-infojus%3ADACF160315%29%20&o=0&f=Total%7CTipo%20de%20Documento/Doctrina%7CFecha%7COrganismo%7CPublicaci%F3n%7CTribunal%7CTema%7CEstado%20de%20Vigencia%7CAutor%7CJurisdicci%F3n&t=1

Enríquez, O. A. M. (2018). Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento. *Revista IUS, 12*(41), 267-291. Recuperado de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472018000100267&lng=es&tlng=es.

Erramouspe, F. D. P. (2010). Delitos informáticos en la legislación argentina. *Actualidad Jurídica, 154*.

Faliero, J. C. (2018). El futuro de la regulación en protección de datos personales en la Argentina. *#LegalTech: el derecho ante la tecnología*, 55-70. Recuperado de https://www.thomsonreuters.com.ar/content/dam/openweb/documents/pdf/arg/white-paper/supl._legaltech_preplanta.pdf

Farias, C. C., Rosenvald, N., y Braga, F. N (2016). *Curso de Direito Civil: responsabilidade civil* [Curso de Derecho Civil: Responsabilidad Civil]. Salvador: Juspodivm.

Farias, L., y Monteiro, T. (2012). *A identidade adquirida nas redes sociais através do conceito de persona* [La identidad adquirida en las redes sociales a través del concepto de persona]. En *XIX Prêmio Expocom* (pp. 1-11). Sâo Paulo: Sociedade Brasileira de Estudos Interdisciplinares da Comunicação.

Fernández, D. (2019). La Privacidad Digital. *#Legaltech II - El Derecho Ante La Tecnología,* 63-69. Recuperado de https://www.thomsonreuters.com.ar/content/dam/openweb/documents/pdf/arg/white-paper/suplemento-legal-tech-ii-thomsonreuters.pdf

Fernández, E. H. S. F. (2014). El artículo 42 de la Constitución Nacional veinte años después y a propósito de la reciente sanción del Código Civil y Comercial. *Thomson Reuters*, 1-6. Recuperado de http://www.derecho.uba.ar/institucional/pacem/pdf/ferrer-de-fernandez-el-articulo-42-de-la-constitucion-nacional.pdf.

Fernandéz, F. R. (2020). El acceso a los datos y contenidos gestionados por prestadores de servicios de la sociedad de la información de personas

fallecidas: análisis de los límites. *Métodos de Información*, *11*(20), 59-87. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=7547804

Ferraz, M. C. F. (2019). *Volto já (Be right back), de Black Mirror: tecnologias, finitude e a arte de saber terminar* [Vuelvo enseguida (Be right back), de Black Mirror: tecnologías, finitud y el arte de saber terminar]. *Galáxia (São Paulo)*, *41*, 62-74. doi: 10.1590/1982-25542019240169

Ferrero, E., y Schutz, A. (2018). Tráfico de datos personales: su afectación a los derechos personalisimos. *Perspectivas de las Ciencias Económicas y Jurídicas, 3*(2), 55-74. doi: 10.19137/perspectivas-2013-v3n2a03

Font, J. L. O., y Boff, S. O. (2019). La disposición *post mortem* de los bienes digitales: especial referencia a su regulación en América Latina. *Derecho PUCP*, *83*, 29-60. doi: 10.18800/derechopucp.201902.002

Frazão, A. (12 de septiembre de 2018). *Nova LGPD: A importância do consentimento para o tratamento dos dados pessoais* [Nueva LGPD: la importancia del consentimiento para el tratamiento de datos personales]. [Mensaje de Blog]. Recuperado de: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-a-importancia-do-consentimento-para-o-tratamento-dos-dados-pessoais-12092018.

Garsco, M. A. (2015). El nuevo Código Civil y Comercial respecto del derecho a la imagen, y de la propiedad intelectual en el régimen patrimonial de las relaciones de familia. *ElDial.com*, 1-10. Recuperado de https://www.pensamientocivil.com.ar/system/files/2015/10/Doctrina2080.pdf.

Ghosh, P. (10 de febrero de 2020). *A indústria de robôs sexuais é uma ameaça à sociedade?* [¿Es la industria de los robots sexuales una amenaza para la

sociedad?]. [Publicación de BBC]. Recuperado de https://www.bbc.com/portuguese/geral-51557875

Giardelli, G. (2012). *Você é o que você compartilha: e-agora: como aproveitar as oportunidades de vida e trabalho na sociedade em rede* [Eres lo que compartes: e-agora: cómo aprovechar las oportunidades de vida y trabajo en la sociedad en red]. São Paulo: Gente.

Góis, A. A. (2017). *A eficácia do cadastro positivo e o direito à privacidade* [La eficacia del registro positivo y el derecho a la privacidad]. *Âmbito Jurídico*, *20*(158). Recuperado de http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=18578&revista_caderno=9

Gonçalves, T. C. N. M., y Varella, M. D. (2018). *Os desafios da administração pública na disponibilização de dados sensíveis* [Desafíos de la administración pública para poner a disposición datos sensibles]. *Revista Direito GV*, *14*(2), 513-536. doi: 10.1590/2317-6172201821

Hartmann, M., y Wimmer, J. E. (2011). *Digitale Medientechnologien: Vergangenheit – Gegenwart – Zukunft* [Tecnologías de medios digitales: pasado - presente - futuro]. Wiesbaden: VS.

Henrÿ, H. (2017). La revalorización de los datos personales – ¡una genuina tarea de las cooperativas! En G. G. García (ed.), *Empleo, innovación e inclusión en la economía social: problemática jurídica y social* (pp. 109-114). Valencia: Edita CIRIEC.

Herrera, M. (2015). *Código Civil y Comercial de la Nación comentado* (1a ed.). Ciudad Autónoma de Buenos Aires: Infojus.

Honorato, G., y Leal, L. T. (2020). *Exploração econômica de perfis de pessoas falecidas: reflexões jurídicas a partir do caso Gugu Liberato* [Explotación económica de perfiles de personas fallecidas: reflexiones jurídicas basadas en el caso Gugu Liberato]. *Revista Brasileira de Direito Civil, 23*, 155-173. doi:10.33242/rbdc.2020.01.008

Iglesias, G. (2011). Inviolabilidad de la correspondencia y comunicaciones electrónicas en el derecho argentino. *Revista Iberoamericana El Derecho Informático, 10*. Recuperado de https://ar.ijeditores.com/articulos.php?idarticulo=65956&print=1

Iglesias, G. (2015). La responsabilidad de los buscadores de Internet después del caso Belen Rodriguez. En *15º Simposio Argentino de Informática y Derecho* (pp. 131-145). Rosário, Argentina.

Imbernón, N. M. (2020). El testamento digital en la nueva Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantia de los derechos digitales. *Anuario de Derecho Civil, 73* (1), 241-281. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=7504469

Iturralde, M. E. (2019). *Políticas de comunicación en ciudades intermedias: el proceso de discusión, sanción y aplicación de la Ley de Servicios de Comunicación Audiovisual en Azul, Olavarría y Tandil* (Tesis de Doctorado). Universidad Nacional de la Plata, Argentina. Recuperado de http://sedici.unlp.edu.ar/handle/10915/73762

Juri, Y. E (2019). Protección de datos personales: especial referencia al proyecto de reforma de la ley Argentina Nº 25.326. *Revista de Derecho, Ciencias Sociales y Políticas*, *25,* 221-231. Recuperado de https://www.rduss.com/index.php/rduss/article/view/355

Kahansky, C. M. R. (2019). *Vigencia del derecho europeo de protección de datos personales (*Tesis de Doctorado). Programa de Doctorado en Unión Europea. Recuperado de http://e-spacio.uned.es/fez/eserv/tesisuned:ED-Pg-UniEuro-Cmreyes/REYES_KAHANSKY_Carolina_Marcela_Tesis.pdf

Keller, D. (2017). *El "derecho al olvido" de Europa en América Latina*. Hacia una Internet libre de censura II: Perspectivas en América Latina/Agustina Del Campo, 171-198. Compilado por Agustina Del Campo.-1a ed.- Buenos Aires: Universidad de Palermo – UP. Recuperado de https://www.palermo.edu/cele/pdf/investigaciones/Hacia_una_internet_libre_de_censura_II.pdf

Kemp, S. (21 de julio de 2020a). *More than half of the people on earth now use social media* [Más de la mitad de la población mundial usa ahora las redes sociales]. [Publicación de DatarePortal]. Recuperado de https://datareportal.com/reports/more-than-half-the-world-now-uses-social-media

Kemp, S. (17 de febrero de 2020b). Digital 2020: Argentina [Publicación de DatarePortal]. Recuperado de https://datareportal.com/reports/digital-2020-argentina

Kemp, S. (17 de febrero de 2020c). *Digital 2020: Brazil* [Digital 2020: Brasil]. [Publicación de DatarePortal]. Recuperado de https://datareportal.com/reports/digital-2020-brazil

Kemp, S. (21 de julio de 2020d). *Digital 2020: july global statshot* [Digital 2020: estadística global de julio]. [Publicación de DatarePortal]. Recuperado de https://datareportal.com/reports/digital-2020-july-global-statshot

Kemp, S. (27 de enero de 2021a). *Digital 2021: The Latest Insights Into The 'State Of Digital'* [Digital 2021: Los Últimos Conocimientos Sobre El 'Estado De Lo Digital'] [Publicación de DatarePortal]. Recuperado de https://wearesocial.com/blog/2021/01/digital-2021-the-latest-insights-into-the-state-of-digital

Kemp, S. (11 de febrero de 2021b). Digital 2021: Argentina [Publicación de DatarePortal]. Recuperado de https://datareportal.com/reports/digital-2021-argentina

Kemp, S. (11 de febrero de 2021c). *Digital 2021: Brazil* [Digital 2021: Brasil]. [Publicación de DatarePortal]. Recuperado de https://datareportal.com/reports/digital-2021-brazil

Lee, K. (2019). *Inteligência Artificial: como os robôs estão mudando o mundo, a forma como amamos, nos comunicamos e vivemos* [Inteligencia artificial: cómo los robots están cambiando el mundo, la forma en que amamos, nos comunicamos y vivimos]. Rio de Janeiro: Globo Livros.

Leister, A. C. C. C., y Wang, D. W. L. (2014). *Metodologia Jurídica: um roteiro prático para os trabalhos de conclusão de curso* [Metodología Jurídica: una hoja de ruta práctica para el trabajo de finalización del curso]. São Paulo: Saraiva.

Lipszyc, D. (1993). *Derechos de autor y derechos conexos.* Buenos Aires: Ediciones Unesco-Cerlac-Zavalía.

Lopes, C. G., y Vas, B. B. (2016). *O ensino de história na palma da mão: o Whatsapp como ferramenta pedagógica para além da sala de aula* [La enseñanza de la historia en la palma de su mano: Whatsapp como herramienta pedagógica más allá del aula]. En *Simpósio Interncional de*

Educação à Distância. (pp. 1-14). Sâo Carlos, São Paulo: Universidade Federal de São Carlos.

López, N., Maranhão, J., Campos, R., y Abrusio, J. (23 de septiembre de 2020). *A vigência da LGPD e o desafio de adequação no Brasil e do Brasil* [La vigencia de la LGPD y el desafío de la adaptación en Brasil y del Brasil]. [Publicación de Consultor Jurídico]. Recuperado de https://www.conjur.com.br/2020-set-23/direito-digitala-vigencia-lgpd-desafio-adequacao-brasil-brasil

Lorenzetti, P. (2015). Compatibilización entre la esfera pública y la privada y entre el ámbito colectivo y el individual, en el Código Civil y Comercial de la Nación. *Jurisprudencia Argentina*, *14*, 3-24. Recuperado de http://estudiolorenzetti.com.ar/wp-content/uploads/2015/10/Compatibilizacion-entre-la-esfera-publica-y-la-privada-Pablo-Lorenzetti.pdf

Luz, P. H. M. (2019). *Direito ao esquecimento no Brasil* [Derecho al olvido en Brasil]. Curitiba: GEDAI/UFPR.

Maichaki, M. R. (2018). *Herança digital: O precedente alemão e os direitos fundamentais à intimidade e privacidade* [Herencia digital: el precedente alemán y los derechos fundamentales a la intimidad y la privacidad]. *Revista Brasileira de Direito Civil em Perspectiva*, *4*(2), 136-155. Recuperado de https://core.ac.uk/download/pdf/210567288.pdf

Manchini, C. P. C., Augusto, J. G. S., y Franceschet, J. C. (2020). *O direito à honra post mortem: limitações e avanços no direito brasileiro à luz da gestão de conflitos* [El derecho al honor *post mortem*: limitaciones y avances del derecho brasileño a la luz de la gestión de conflictos]. En *Encontro virtual do CONPEDI* (pp. 86-106). Florianópolis: CONPEDI.

Masciotra, M. (2018). Protección de datos personales y su integración en el marco de los derechos humanos [Publicación de SAIJ]. Recuperado de http://www.saij.gob.ar/mario-masciotra-proteccion-datos-personales-su-integracion-marco-derechos-humanos-dacf180264-2018-12-10/123456789-0abc-defg4620-81fcanirtcod?q=fecha-rango%3A%5B20180918%20TO%2020190318%5D&o=12&f=Total%7CFecha%7CEstado%20de%20Vigencia%5B5%2C1%5D%7CTema%5B5%2C1%5D%7COrganismo%5B5%2C1%5D%7CAutor%5B5%2C1%5D%7CJurisdicci%F3n%5B5%2C1%5D%7CTribunal%5B5%2C1%5D%7CPublicaci%F3n%5B5%2C1%5D%7CColecci%F3n%20tem%E1tica%5B5%2C1%5D%7CTipo%20de%20Documento/Doctrina&t=60

Masili, C. M. V. (2018). *Regulação do uso de dados pessoais no Brasil: papel do usuário na defesa de um direito à tutela de dados pessoais autônomo* [Regulación del uso de datos personales en Brasil: el papel del usuario en la defensa del derecho a la protección de datos personales autónomos]. (Tesis de Maestría). Universidade de Brasília, Brasília. Recuperado de https://repositorio.unb.br/bitstream/10482/34290/3/2018_ClarissaMenezesVazMasili.pdf

Maurino, G. (2008). Pobreza, constitución y democracia: Aportes desde la autonomía personal [Publicación de blog]. Recuperado de https://www.academia.edu/5014214/POBREZA_CONSTITUCI%C3%93N_Y_DEMOCRACIA_APORTES_DESDE_LA_AUTONOM%C3%8DA_PERSONAL

Mejía R., y Palmero, A. (2019). La Secretaría de Gobierno de Salud de la Nación regula el acceso a los datos de salud con fines de investigación. *Revista Argentina de Salud Pública, 10*(40), 5-6. Recuperado de http://rasp.msal.gov.ar/rasp/articulos/volumen40/5-6.pdf

Mendes, L. S. (2014). *Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental* [Privacidad, protección de datos y defensa del consumidor: pautas generales para un nuevo derecho fundamental]. São Paulo: Saraiva.

Mendes, L., y Fonseca, G. (2020). *Proteção de dados para além do consentimento: tendências contemporâneas de materialização* [Protección de datos más allá del consentimiento: tendencias contemporáneas de materialización]*. Revista Estudos Institucionais, 6*(2), 507-533. doi: https://doi.org/10.21783/rei.v6i2.521

Mezzaroba, O. (2017). *Manual de metodologia da pesquisa no Direito* [Manual de metodología de la investigación en Derecho] (7a ed.). São Paulo: Saraiva.

Molina Quiroga, E. (2017). Redes sociales, derechos personalísimos y la libertad de expresión. La Ley. Recuperado de http://www.laleyonline.com.ar

Molina Quiroga, E. (2018). Responsabilidad de los buscadores en Internet: libertad de expresión y función preventiva de la responsabilidad. *#LegalTech: el derecho ante la tecnología*, 163-185. Recuperado de https://www.thomsonreuters.com.ar/content/dam/openweb/documents/pdf/arg/white-paper/supl._legaltech_preplanta.pdf

Palma, J. B., Feferbaum, M., y Pinheiro, V. M. (2014). *Metodologia Jurídica: um roteiro prático para os trabalhos de conclusão de curso* [Metodología Jurídica: una hoja de ruta práctica para el trabajo de finalización del curso]. São Paulo: Saraiva.

Palomo, L., Piccardi, L. S., y Guillet, S. M. (2020). Guía de recomendaciones para el tratamiento del big data como evidencia digital. En *XXII Workshop de*

Investigadores en Ciencias de la Computación (pp. 205-209). El Calafate, Santa Cruz: Universidade Nacional de la Plata.

Pérez Luño, A. (1996) *Manual de informática y derecho*. Barcelona: Ariel.

Perinotto, A. R. C., Alves, C. E. S., Silva, L. F., y Vieira, V. B. (2020). *O espaço turístico de Parnaíba-PI nas fotografias on-line, por meio das hashtags #parnaiba e #deltadoparnaiba: uma análise na rede social Instagram* [El espacio turístico de Parnaíba-PI en fotografías online, utilizando los *hashtags* #parnaiba y #deltadoparnaiba: un análisis en la red social *Instagram*]. *Revista Acadêmica Observatório de Inovação do Turismo, 14*(1), 1-22. doi: 10.17648/raoit.v14n1.5570

Petrino, R. V. (2013). Artículo 11. Protección de la honra y de la dignidad. En R. M. A. Regueira (ed.), *La Convención Americana de Derechos Humanos y su proyeccíon em el Derecho argentino* (pp. 203-218). Buenos Aires: La Ley.

Piana, R. S., y Amosa, F. M. (2018). El derecho de acceso a la información pública en la provincia de Buenos Aires. *Revista Derechos en Acción, 6*(6). doi:10.24215/25251678e124

Piton, A. C. (2017). *Análise das consequências jurídicas da violação nas mídias sociais, do direito de imagem, honra, intimidade e privacidade, na perspectiva do direito civil brasileiro* [Análisis de las consecuencias jurídicas de la violación en las redes sociales, el derecho a la imagen, el honor, la intimidad y la privacidad, desde la perspectiva del derecho civil brasileño]. *Revista Âmbito Jurídico*, *158*. Recuperado de https://ambitojuridico.com.br/cadernos/direito-civil/analise-das-consequencias-juridicas-da-violacao-nas-midias-sociais-do-direito-de-imagem-honra-intimidade-e-privacidade-na-perspectiva-do-direito-civil-brasileiro/

Placzek, T. (2006). *Allgemeines Persönlichkeitsrecht und privatrechtlicher Informations – und Datenschutz* [Derechos personales generales y protección de la información y datos de derecho privado]. Hamburg: Lit.

Ponte, J. V. C. (2020). *A influência da interface da rede social Facebook na homofobia e na comunidade LGBTI+* [La influencia de la interfaz de la red social *Facebook* en la homofobia y la comunidad *LGBTI+*]. [Publicación de Academia.edu]. Recuperado de https://www.academia.edu/43286910/A_Influ%C3%AAncia_da_Interface_da_Rede_Social_facebook_na_Homofobia_e_na_Comunidade_LGBTI

Porcelli, M. P. (2017). (Des)Protección del derecho de autor en la era digital: principales tendencias legislativas, doctrinarias y jurisprudenciales argentinas sobre la denominada “piratería informática”. *Quaestio Iuris, 10*(4), 2339-2376. doi: 10.12957/rqi.2017.22281

Puccinelli, O. (2019). El derecho al olvido digital: la nueva cara de un derecho tan viejo como polémico. *Revista Derecho Constitucional,1*, 78-91. doi: 10.37767/2683-9016(2019)006

Queiroz, R. M. R. (2011). *Artigo científico: concepção, temas, métodos e técnicas* [Artículo científico: concepción, temas, métodos y técnicas]. *BePress Selected Works*, 1-28. Recuperado de https://works.bepress.com/rafaelmafei/10/download/

Rallo, A. (2016). El debate europeo sobre el derecho al olvido en internet. *Revista Latinoamericana de Protección de Datos Personales, 3*, 19-48.

Ramírez, M. S. M., y Vignau, A. B. (2019) *Democracia, privacidad y protección de datos personales*. Ciudad de México: Instituto Nacional Electoral.

Recuperado de https://www.ine.mx/wp-content/uploads/2020/02/cuaderno_41.pdf

Reani, V. (21 de septiembre de 2018). *O impacto da lei de proteção de dados brasileira nas relações de trabalho* [El impacto de la ley brasileña de protección de datos en las relaciones laborales]. [Publicación de Consultor Jurídico]. Recuperado de https://www.conjur.com.br/2018-set-21/valeria-reani-alei-protecao-dados-relacoes-trabalho

Remolina Angarita, N. (2017) *¿Derecho al olvido en el ciberespacio? Principios internacionales y reflexiones sobre las regulaciones latinoamericanas.* Hacia una Internet libre de censura II: Perspectivas en América Latina/Agustina Del Campo. Compilado por Agustina Del Campo, 199-226.-1a ed.- Buenos Aires: Universidad de Palermo – UP. Recuperado de https://www.palermo.edu/cele/pdf/investigaciones/Hacia_una_internet_libre_de_censura_II.pdf

Retondo, F. (2016). El derecho al olvido ¿existe?. *Revista Latinoamericana de Protección de Datos Personales, 3*, 83-118. Buenos Aires: Duken.

Rezende, L. V. R., y Lima, M. R. (2016). *Governança na internet: um estudo sobre o marco civil brasileiro* [Gobernanza de Internet: un estudio sobre el marco civil brasileño]. *Palabra Clave [online], 19*(1), 133-155. doi: 10.5294/pacla.2016.19.1.6.

Ribeiro, S. L. A. (2015). El silencio del badajo: las redes sociales, el marco civil y el habeas data como instituto de protección de la vida privada frente a los avances tecnológicos. *Revista UNIFESO,2*(2), 24-63. Recuperado de http://www.revista.unifeso.edu.br/index.php/revistaunifesohumanasesociais/article/view/44/50

Riquert, M. A. (2008). "Algo más sobre la legislación contra la delincuencia informática en Mercosur a propósito de la modificación al Código Penal Argentino por Ley 26.388". *Revista de Derecho Informático*, *121.* Recuperado de http://www.ciidpe.com.ar/area2/DELINCUENCIA%20INFORMATICA.RIQUERT.pdf

Rocha, C. (2 de março de 2017). *App permite falar e até tirar selfie com quem já morreu* [Aplicación permite hablar e incluso hacerte una *selfie* con alguien que ha muerto]. [Publicación de Olhar Digital]. Recuperado de https://olhardigital.com.br/noticia/app-permite-falar-e-ate-tirar-selfie-com-quem-ja-morreu/66536

Rodovalho, J. P. (2021). *Proteção de dados nas relações de emprego: a prevenção da empresa depois da LGPD* [Protección de datos en las relaciones laborales: prevención de la empresa después de LGPD]. Londrina: Thoth.

Rodrigues, J. G. (2014). *Publicidade, transparência e abertura na administração pública* [Publicidad, transparencia y apertura en la administración pública]. *Revista de Direito Administrativo (RDA), 266*, 89-123. doi: 10.12660/rda.v266.2014.32142

Saltor, C. E (2013). *La protección de datos personales: estudio comparativo Europa-América com especial análisis de la situación Argentina* (Tesis de Doctorado). Universidad Complutense de Madrid, Madrid. Recuperado de https://eprints.ucm.es/22832/

Santiago, F. (21 de septiembre de 2018). *Lei de proteção de dados muda funcionamento de empresas* [Ley de protección de datos cambia la forma en que operan las empresas]. [Publicación de Consultor Jurídico].

Recuperado de https://www.conjur.com.br/2018-ago-20/fernando-santiago-lei-protecao-dados-muda-atuacao-empresas

Schiavo, N. (2020). ¿Debemos excluir la exclusión? *La Ley*, año LXXXIV, Tomo 2020-E, n. 153, publicado en 19/08/2020.

Schreiber, A. (2011). *Direitos da personalidade* [Derechos de personalidad]. São Paulo: Atlas.

Schwab, K. (2016). *A Quarta Revolução Industrial* [La cuarta revolución industrial]**.** São Paulo: Edipro.

Seminario, M. (20 de mayo de 2020) ¿Cómo tratar los datos personales de una persona fallecida? [Mensaje de Blog]. Recuperado de https://protecciondatos-lopd.com/empresas/datos-personales-persona-fallecida/

Short, J. E, y Todd, S. (2017). *What's Your Data Worth?* [¿Cuál es el valor de sus datos?]. *Mit Sloan Management Review, 58*(3), 16-20. Recuperado de https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/short-whats-your-data-worth.pdf

Silva, I. G. (2020). *Isso é muito Black Mirror: narcisismo digital e vigilância algorítmica na composição da crise ética contemporânea* [Esto es muy *Black Mirror*: narcisismo digital y vigilancia algorítmica en la composición de la crisis ética contemporánea]. (Tesis de Maestría). Universidade Federal do Rio Grande Do Norte, Natal. Recuperado de https://repositorio.ufrn.br/jspui/bitstream/123456789/29172/1/IssomuitoBlack_Silva_2020.pdf

Silva, J. A (2018). *Curso de Direito Constitucional Positivo* [Curso de Derecho Constitucional positivo]. São Paulo: Malheiros.

Silva, M. A., y Carvalho, I. D. Jr. (2020). *Youtube como rede social: contribuições da plataforma para a aprendizagem de língua inglesa* [*Youtube* como red social: aportes de la plataforma para el aprendizaje del idioma inglés]. *Revista Percursos Linguísticos, 10(*24), 126-147. Recuperado de https://periodicos.ufes.br/percursos/article/view/28964

Silva, S. A. A., Maia, L. C. G., Rafacho, L. R., Pereira, A. L. O., y Alto, P. S. M. (2020). *Herança da informação digital e direito ao esquecimento em redes sociais on-line: uma revisão sistemática de literatura* [Herencia de la información digital y derecho al olvido en las redes sociales online: una revisión sistemática de la literatura]. *Em Questão, 26*(1), 375-401. doi: 10.19132/1808-5245261.375-401

Silva, U. H., y Doto, V. C. (2017). *Um olhar digital: aplicativos que interagem com "pessoas" após a morte: uma análise sobre as novas tecnologias e as violações da dignidade humana no uso da imagem post mortem* [Una mirada digital: aplicaciones que interactúan con "personas" después de la muerte: un análisis de las nuevas tecnologías y las violaciones de la dignidad humana en el uso de imágenes *post mortem*]. En *X Encontro Internacional de Produção Científica*. Maringá: UniCesumar.

Silva, V. R. B. S. (2015). *Preocupação com a privacidade na internet: uma pesquisa exploratória no cenário brasileiro* [Preocupación por la privacidad en Internet: una investigación exploratoria en el escenario brasileño]. (Tesis de Maestría). Pontifícia Universidad Católica del Rio Grande do Sul, Porto Alegre. Recuperado de http://tede2.pucrs.br/tede2/handle/tede/6018

Silveira, M. A. K. (2013). *Lei de Acesso a Informações Públicas (Lei n. 12.527/2011): democracia, república e transparência no Estado constitucional* [Ley de Acceso a la Información Pública (Ley n. 12.527/2011): democracia, república y transparencia en el estado constitucional]. *Revista dos Tribunais, 102*(927), 131-155. Recuperado de https://dspace.almg.gov.br/handle/11037/22011

SIlveira, S. A., Avelino, R., y Souza, J. (2016). *A privacidade e o mercado de dados pessoais* [Privacidad y mercado de datos personales]. *Liinc Em Revista*, *12*(2). https://doi.org/10.18617/liinc.v12i2.902.

Souza, L. R. M. (2018). *Proteção de dados pessoais: estudo comparado do Regulamento 2016/679 do Parlamento europeu e conselho e o projeto de lei brasileiro n. 5.276/2016* [Protección de datos personales: estudio comparativo del Reglamento 2016/679 del Parlamento Europeo y del consejo y el proyecto de ley brasileño n. 5.276/2016]. *Caderno Virtual*, 1-104. Recuperado de https://www.portaldeperiodicos.idp.edu.br/cadernovirtual/article/download/3153/1484

Spina, M. V; Giler, S. (2019). La autonomía de la voluntad en el derecho sucesorio y la protección de personas vulnerables. *41ª Jornada Notarial Bonaerense.* Recuperado de http://www.jnb.org.ar/41/images/41-trabajos/tema-2/2-SPINA-Marcela-Viviana-GILER-Silvia.pdf

Tanús, G. D. (2002). Proteccion de datos personales. Principios generales, derechos, deberes y obligaciones [Publicación de PDP]. Recuperado de http://www.protecciondedatos.com.ar/doc7.htm

Teixeira, A. D., y Paula, R. (2017). *Direito ao esquecimento em herança digital* [Derecho al olvido en la herencia digital]. *JUDICARE*, *11(*1), 31-47.

Recuperado de http://www.ienomat.com.br/revista/index.php/judicare/article/download/19/18/

Tomasevicius, E. F. (2016). *Marco civil da internet: uma lei sem conteúdo normativo* [Marco civil de internet: una ley sin contenido normativo]. *Estudos Avançados*, *30*(86), 269-285. Recuperado de http://www.revistas.usp.br/eav/article/view/115093

Turnes, Y. (2016). Delitos informáticos: especial atención a las leyes 26.388 y 26.904 (Tesis de Doctorado). Universidad Siglo 21. Recuperado de https://repositorio.uesiglo21.edu.ar/handle/ues21/14467

Vercelli, A. (2019). *Facebook Inc*. *Cambridge Analytica*: (un)protection of personal data and global disinformation campaigns. *Electronic Journal of SADIO (EJS)*, *18*(2), 57-70. Recuperado de https://47jaiio.sadio.org.ar/index.php/EJS/article/view/146

Villalba, C. A. y Lipszyc, D. (2001). *El derecho de autor en la Argentina.* Buenos Aires: Editorial La Ley.

Villegas Carrasquilla, L. (2012). *Protección de datos personales en América Latina: retención y tratamiento de datos personales en el mundo de Internet.* Compilado por Eduardo Andrés Bertoni.-1a ed, 125-164. Buenos Aires: Universidad de Palermo - UP. Recuperado de https://www.palermo.edu/cele/pdf/internet_libre_de_censura_libro.pdf

Viola, M., Doneda, D., Córdova, Y, y Itagiba, G. (2016). *Entre privacidade e liberdade de informação e expressão: existe direito ao esquecimento no Brasil?* [Entre la privacidad y la libertad de información y expresión: ¿existe el derecho al olvido en Brasil?]. En G. Tepedino, A. C. B. Teixeira, y V.

Almeida (Coords.). *O Direito Civil entre o sujeito e a pessoa: estudos em homenagem ao professor Stefano Rodotà* (pp. 361-380). Belo Horizonte: Fórum.

Westin, A. (1970). *Privacy and freedom* [Privacidad y libertad]. NewYork: Atheneum.

Zampier, B. (2021). *Bens digitais: cybercultura, redes sociais, e-mails, músicas, livros, milhas aéreas, moedas virtuais* [Bienes digitales: cibercultura, redes sociales, correos electrónicos, música, libros, millas aéreas, monedas virtuales] (2a ed.). Indaiatuda: Foco.

Fuentes de información

Agencia de Acceso a la Información Pública (2018). Cuadro comparativo: Ley 25.326 de Protección de Datos Personales e Mensaje 147/2018 Proyecto de Ley de Protección de Datos Personales. *Direción Nacional de Protección de Datos Personales*. Recuperado de https://www.argentina.gob.ar/sites/default/files/comparativo_ley_datos.pdf

Agencia de Acceso a la Información Pública (5 de septiembre de 2019). *Cuánto sabemos de datos personales* [Publicación de Argentina.gob.ar]. Recuperado de: https://www.argentina.gob.ar/noticias/cuanto-sabemos-de-datos-personales

Argentina (2014). *Código Civil y Comercial de la Nación* (1ª ed.). Ciudad Autónoma de Buenos Aires: Infojus

Argentina (2016). *Convención Americana sobre Derechos Humanos* (1a ed.). Ciudad Autónoma de Buenos Aires: Ministerio de Justicia y Derechos Humanos de la Nación. Secretaría de Derechos Humanos y Pluralismo

Cultural. Recuperado de https://www.argentina.gob.ar/sites/default/files/derechoshumanos_publicaciones_colecciondebolsillo_10_convencion_americana_ddhh.pdf

BBC News Brasil (19 de febrero de 2020). *Mãe 'encontra' filha morta com ajuda de realidade virtual em programa de TV* [Madre 'encuentra' a su hija muerta con ayuda de realidad virtual en programa de televisión]. [Publicación de BBC]. Recuperado de https://www.bbc.com/portuguese/internacional-51551583

Brand Finance (2020). *Global 500 2020 Ranking* [Publicación de Brand Finance]**.** Recuperado de https://brandirectory.com/rankings/global/table.

Brooker, C. (Director). (2013). *Black Mirror: Be Right Back* [*Black Mirror:* Vuelvo enseguida]. [serie]. Netflix.

Cámara Nacional de Apelaciones en lo Civil y Comercial Federal, Sala III, 22/04/2016, “F., D. S. c. Google Inc. y otro s/ medidas cautelares–incidente”.

Cámara Nacional en lo Criminal y Correccional, Sala I, 19/05/2020, “G., E. D. s/ Nulidad”. *Repertorio La Ley, 2020*, 7-8, año LXXXIV, nº 153, Publicado al 19/08/2020.

Constituição da República Federativa do Brasil (1988). Recuperado de http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

Conferencia Internacional Americana (1948). Declaración Americana de los Derechos y Deberes del Hombre. Recuperado de http://www.infoleg.gob.ar/?page_id=1000

Corte Suprema de la Nación Argentina, Fallos: Fallos: 306:1892, 11/12/1984, "*Ponzetti de Balbín, Indalia c/ Editorial Atlántida S.A. s/ daños y perjuicios*.". Recuperado de http://www.saij.gob.ar/descarga-archivo?guid=rstuvwfa-llos-comp-uest-o84000564pdf&name=84000564.pdf

Corte Suprema de la Nación Argentina, Fallos: 330:4615, 30/10/2007, "Franco, Julio César c/ Diario "La Mañana" y/u otros s/ daños y perjuicios". Recuperado de http://sjconsulta.csjn.gov.ar/sjconsulta/documentos/verDocumentoById.html?idDocumento=6351172&cache=1520294500001

Corte Suprema de la Nación Argentina, H. 270, XLII., "Halabi, Ernesto c/ P.E.N - ley 25. dto. 1563/04 s/ amparo ley 16.986". Recuperado de https://sjconsulta.csjn.gov.ar/sjconsulta/documentos/verDocumentoByIdLinksJSP.html?idDocumento=6625571&cache=1620503669224

Corte Suprema de la Nación Argentina, R. 522, XLIX, "Rodriguez, María Belén c/ Google Inc y otro y otros s/daños y perjuicios". Recuperado de https://sjconsulta.csjn.gov.ar/sjconsulta/documentos/verDocumentoByIdLinksJSP.html?idDocumento=7162581&cache=1532970625515

Corte Suprema de la Nación Argentina, Fallos: 337:921, 05/08/2014, "*Recurso de hecho deducido por la demandada en la causa Irigoyen, Juan Carlos Hipólito c/ Fundación Wallenberg y otro s/ daños y perjuicios*". Recuperado de http://sjconsulta.csjn.gov.ar/sjconsulta/documentos/verDocumentoById.html?idDocumento=7131214&cache=1513209800001

Decreto n. 151, de 18 de enero de 1974. Reglamentacion del Decreto-Ley 20.216/73. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do%3Bjsessionid=D87676BF1F91A219ABFAC32A582AC319?id=248809

Decreto n. 1187, de 10 de junio de 1993. Régimen postal, registro nacional de prestadores de servicios postales, publicidad del servicio y responsabilidad frente al cliente y disposiciones generales. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/10000-14999/13490/norma.htm

Decreto n. 554, de 18 de junio de 1997. Declárase de Interés Nacional el acceso de los habitantes de la República Argentina a la red mundial INTERNET. Autoridad de Aplicación. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/44083/norma.htm

Decreto n. 1279, de 25 de noviembre de 1997. Declárase comprendido en la garantía constitucional que ampara la libertad de expresión al servicio de INTERNET. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/45000-49999/47583/norma.htm

Decreto n. 311, de 24 de marzo de 2020. Emergencia sanitaria. Abstención de corte de Servicios en caso de mora o falta de pago. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/335000-339999/335827/norma.htm

Decreto n. 690, de 21 de agosto de 2020. Argentina Digital. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/340000-344999/341372/norma.htm

Decreto-Ley n. 20.216, de 32 de marzo de 1973. Ley de correos. Recuperado de: http://servicios.infoleg.gob.ar/infolegInternet/anexos/20000-24999/21843/norma.htm

Facebook (2020a). *Política de dados* [Política de datos]. Recuperado de https://www.facebook.com/privacy/explanation

Facebook (2020b). *Central de ajuda: o que acontecerá com minha conta do facebook se eu falecer?* [Centro de ayuda: ¿Qué pasará con mi cuenta de Facebook si muero?]. Recuperado de https://pt-br.facebook.com/help/103897939701143/

Facebook (2020c). *Central de ajuda: o que é um contato herdeiro e o que ele pode fazer com minha conta do Facebook?* [Centro de ayuda: ¿Qué es un contacto heredero y qué puede hacer con mi cuenta de Facebook?]. Recuperado de https://pt-br.facebook.com/help/1568013990080948

Google (2020a). *Privacidade e Termos* [Privacidad y Términos]. Recuperado de: https://policies.google.com/privacy?hl=pt-BR&gl=br

Google (2020b). *Tecnologias* [Tecnologías]. Recuperado de https://policies.google.com/technologies/retention?hl=pt-BR&gl=br

Google (2020c). *Ajuda da conta do Google* [Ayuda de la cuenta de Google]. Recuperado de: https://support.google.com/accounts/troubleshooter/6357590?hl=pt-BR#ts=6357650

Instagram (2020a). *Atualizações dos termos e políticas de dados* [Actualizaciones de los términos y políticas de datos]. Recuperado de https://www.instagram.com/terms/accept/?hl=pt-br

Instagram (2020b). *Políticas de dados do Instagram* [Políticas de datos de *Instagram*]. Recuperado de https://help.instagram.com/519522125107875.

Instagram (2020c). *Termos de uso* [Terminos de uso]. Recuperado de https://help.instagram.com/581066165581870

Instagram (2020d). *Como faço para denunciar a conta de uma pessoa falecida no Instagram?* [¿Cómo denuncio la cuenta de *Instagram* de una persona fallecida?]. Recuperado de https://pt-br.facebook.com/help/instagram/264154560391256

Instagram (2020e). *O que acontece quando a conta do Instagram de uma pessoa falecida é transformada em memorial?* [¿Qué sucede cuando la cuenta de Instagram de una persona fallecida se convierte en un monumento?]. Recuperado de https://help.instagram.com/231764660354188

Lei Complementar n. 166, de 8 de abril de 2019. Altera a Lei Complementar nº 105, de 10 de janeiro de 2001, e a Lei nº 12.414, de 9 de junho de 2011, para dispor sobre os cadastros positivos de crédito e regular a responsabilidade civil dos operadores [Modifica la Ley Complementaria n. 105, de 10 de enero de 2001, y la Ley n. 12.414, de 9 de junio de 2011, para establecer antecedentes crediticios positivos y regular la responsabilidad civil de los operadores.]. Recuperado de http://www.planalto.gov.br/ccivil_03/leis/lcp/Lcp166.htm

Lei n. 10.406, de 10 de janeiro de 2002. Intitui o Código Civil [Instituye el Código Civil]. Recuperado de http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm

Lei n. 12.414, de 9 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito [Disciplina la formación y consulta de bases de datos con información sobre

incumplimiento, personas naturales o jurídicas, para la formación de historial crediticio]. Recuperado de http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm#:~:text=Convers%C3%A3o%20da%20Medida%20Provis%C3%B3ria%20n%C2%BA%20518%2C%20de%202010.&text=Disciplina%20a%20forma%C3%A7%C3%A3o%20e%20consulta,forma%C3%A7%C3%A3o%20de%20hist%C3%B3rico%20de%20cr%C3%A9dito..

Lei n. 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências [Regula el acceso a la información prevista en el ítem XXXIII del art. 5, en el punto II del § 3 del art. 37 y en el § 2 del art. 216 de la Constitución Federal; modifica la Ley n. 8.112, de 11 de diciembre de 1990; deroga la Ley n. 11.111, de 5 de mayo de 2005, y disposiciones de la Ley N ° 8.159, de 8 de enero de 1991; y hacer otros arreglos]. Recuperado de: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm

Lei n. 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Recuperado de http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

Lei n. 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil [Establece principios, garantías, derechos y deberes para el uso de Internet en Brasil]. Recuperado de http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

Lei n. 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) [Ley General de Protección de Datos Personales (LGPD)]. Recuperado de http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

Lei n. 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências [Dispone sobre protección al consumidor y otras medidas]. Recuperado de http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm

Ley 26.994, de 7 de Octubre de 2014. Código Civil y Comercial de la Nación. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/235975/norma.htm#2

Ley 27.078, de 18 de diciembre de 2014. Tecnologías de la Información y las Comunicaciones. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/239771/norma.htm

Ley n. 24.430, de 3 de enero de 1995. Ordénase la publicación del texto oficial de la Constitución Nacional. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm

Ley n. 25.326, de 30 de octubre de 2000. Disposiciones generales. Principios generales relativos a la protección de datos. Derechos de los titulares de datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Acción de protección de los datos personales. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm

Ley n. 26.032, de 16 de junio de 2005. Servicio de Internet. Establécese que la búsqueda, recepción y difusión de información e ideas por medio del servicio de Internet se considera comprendida dentro de la garantía constitucional que ampara la libertad de expresión. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/105000-109999/107145/norma.htm

Ley n. 26.388, de 24 de junio de 2008. Código Penal. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm

Ley n. 26.529, 19 de noviembre de 2009. Derechos del Paciente en su Relación con los Profesionales e Instituciones de la Salud. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/160000-164999/160432/norma.htm

Ley n. 27.275, de 14 de septiembre de 2016. Derecho de acceso a la información pública. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/265949/norma.htm

Ley n. 27.483, de 6 de diciembre de 2018. Convenios. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/315000-319999/318245/norma.htm

Ley Orgánica n. 3/2018, de 5 de diciembre de 2018. Protección de datos personales y garantía de los derechos digitales. Recuperado de https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673.

Ley n. 11.723, de 26 de septiembre de 1933. Regimen legal de la propiedad intelectual. Recuperado de

http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/42755/texact.htm

Ley n. 27.078, de 18 de diciembre de 2014. Argentina digital**.** Tecnologías de la Información y las Comunicaciones. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/239771/norma.htm

Loi n. 2016-1321, du 7 octobre 2016. Pour une République numérique [Por una República digital]. Recuperado de https://www.legifrance.gouv.fr/jorf/id/JORFARTI000033203260

Naciones Unidas (1948). Declaración Universal de Derechos Humanos. Recuperado de http://www.infoleg.gob.ar/?page_id=1003#:~:text=La%20presente%20Declaraci%C3%B3n%20Universal%20de,estos%20derechos%20y%20libertades%2C%20y

Naciones Unidas (1966). Pacto Internacional de Derechos Civiles y Políticos. Recuperado de https://www.ohchr.org/sp/professionalinterest/pages/ccpr.aspx

Naciones Unidas (1990). Convención sobre los Derechos del Niño. Recuperado de https://www.ohchr.org/sp/professionalinterest/pages/crc.aspx

Mensaje n. 147, de 19 de septiembre de 2018. Proyecto de ley de protección de datos personales [Versión enviada por el Poder Ejecutivo nacional al congreso para someter a su consideración]. Recuperado de: https://www.argentina.gob.ar/sites/default/files/mensaje_ndeg_147-2018_datos_personales.pdf.

OECD (2013). *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value* [Explorando la economía de los datos personales: una encuesta de metodologías para medir el valor monetario]. *OECD Digital Economy Papers*, *220*. doi: 10.1787/5k486qtxldmq-en.

Recomendación Conjunta de la ANPD e outros (2021), de 7 de maio de 2021. Recuperado de https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/recomendacao_whatsapp_-_assinada.pdf

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. *Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)* [Sobre la protección de las personas en lo que respecta al tratamiento de datos personales y la libre circulación de dichos datos y por la que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)]. Recuperado de https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679

Resolución 2814/1997 de la Secretaría de Comunicaciones de Argentina, de 18 de septiembre de 1997. Apruébanse los precios de acceso de la Red Telefónica Pública, que posibilitarán que los clientes de los prestadores de servicios de valor agregado accedan a los servicios de Internet. Recuperado de https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-2814-1997-45977/texto

Resolución 499/1998 de la Secretaría de Comunicaciones de Argentina, de 20 de febrero de 1998. Apruénbanse las tarifas promocionales propuestas por las empresas Telecom Argentina, Stet France Telecom y Telefonica de

Argentina S. A. para los usuarios del servicio básico telefónico a fin de accede al servicio de valor agregado de “Acceso a Internet”. Recuperado de https://www.enacom.gob.ar/multimedia/normativas/1998/Resolucion%20499_98.pdf

Resolución 1235/1998 de la Secretaría de Comunicaciones de Argentina, de 22 de mayo de 1998. Determínase la inscripción que deberán incluir las facturas emitidas por los Internet Provider. Recuperado de https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-1235-1998-51057/texto

Resolución 95/2020 del Senado de la Nación Argentina, de 3 de septiembre de 2020. Declárase la validez del Decreto N° 690/2020. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/340000-344999/341898/norma.htm

Resolución 492/2021 de la Secretaría de Comercio Interior de Argentina, de 14 de mayo de 2021. Filial argentina de *Facebook* y *WhatsApp* - Ordenase. Recuperado de https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-492-2021-349905/texto

Superior Tribunal de Justiça. *Recurso ordinário em mandado de segurança 60531/RO* (2012, 26 de junho) Relator: Ministro Ribeiro Dantas - Terceira Turma. Recuperado de https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201900993927&dt_publicacao=17/12/2020

Superior Tribunal de Justiça. *Recurso especial 1.168.547/RJ* (2010, 11 de mayo) Relator: Ministro Luis Felipe Salomão - Quarta Turma. Recuperado de

https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=200702529083&dt_publicacao=07/02/2011

Superior Tribunal de Justiça. *Recurso especial 1.316.921/RJ* (2012, 26 de junho) Relatora: Ministra Nancy Andrighi - Terceira turma. Recuperado de https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=23036667&num_registro=201103079096&data=20120629&tipo=5&formato=PDF

Superior Tribunal de Justiça. *Recurso especial 1.630.889/DF* (2016, 27 de novembro) Relatora: Ministra Nancy Andrighi. Recuperado de https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=90337966&num_registro=201602636651&data=20181206&tipo=5&formato=PDF

Superior Tribunal de Justiça. *Recurso especial 1.782.212/SP* (2019, 5 de noviembre) Relatora: Ministra Nancy Andrighi - Terceira turma. Recuperado de https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=102950185&num_registro=201702069970&data=20191107&tipo=5&formato=PDF

Superior Tribunal de Justiça. *Recurso especial 1.784.156/SP* (2019, 5 de noviembre) Relator: Ministro Marco Aurélio Bellizze - Terceira turma. Recuperado de https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201803221400&dt_publicacao=21/11/2019

Supremo Tribunal Federal. *Habeas corpus 168052/SP* (2020, 20 de octubre). Relator: Ministro Gilmar Mendes - Segunda Turma. Recuperado de https://jurisprudencia.stf.jus.br/pages/search/sjur437471/false

Supremo Tribunal Federal. *Reclamação 15.955/RJ* (2015, 15 de setembro). Relator: Ministro Celso de Mello – Segunda turma. Recuperado de http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=10241477

Supremo Tribunal Federal. *Recurso extraodinário com agravo* 660.861/MG (2012, 22 de março). Relator: Ministro Luiz Fux. Recuperado de http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=3058915

Supremo Tribunal Federal. *Recurso extraodinário 601314/SP* (2016, 24 de febrero). Relator: Ministro Edson Fachin – Tribunal Pleno. Recuperado de https://jurisprudencia.stf.jus.br/pages/search/sjur356216/false

Supremo Tribunal Federal. *Recurso extraodinário 1010606/RJ* (2021, 11 de febrero). Relator: Ministro Dias Toffoli. Recuperado de http://www.stf.jus.br/portal/diarioJustica/verDiarioProcesso.asp?numDj=31&dataPublicacaoDj=19/02/2021&incidente=5091603&codCapitulo=2&numMateria=2&codMateria=4

Veja (29 de diciembre de 2017). *Todos os episódios de 'Black Mirror', do melhor ao pior* [Todos los episodios de "Black Mirror", del mejor al peor]. [Publicación de Revista Veja]. Recuperado de https://veja.abril.com.br/cultura/todos-os-episodios-de-black-mirror-do-melhor-ao-pior/

We Are Social (2020). *Digital in 2020* [Publicación de wearesocial.com]. Recuperado de: https://wearesocial.com/digital-2020

Whatsapp (2020a). *Sobre o Whatsapp* [Sobre Whatsapp]. Recuperado de https://www.*Whatsapp*.com/about/

Whatsapp (2020b). *Política de privacidade do Whatsapp* [Política de privacidad de Whatsapp]. Recuperado de https://www.Whatsapp.com/legal/#privacy-policy.

Whatsapp (2020c). *Por que o Whatsapp apaga contas inativas* [Por qué Whatsapp elimina las cuentas inactivas]. Recuperado de https://faq.*Whatsapp*.com/general/account-and-profile/about-inactive-account-deletion/?lang=pt_br