Trabajo Final de Graduación

Carrera de Abogacía

La cuestión jurídica del almacenamiento y tratamiento de los datos personales en las llamadas *"cloud computing"* o computación en la nube, en especial su tercerización (outsourcing).

Elba Aurora Mansilla

2018

Resumen

La prestación de servicios de tipo *cloud computing* o computación en la nube ofrece numerosas ventajas económicas y técnicas para distintas organizaciones que se deciden por ella y llevan a cabo su implementación. Esta tesis pretende hacer un recorrido en las leyes nacionales y evaluar el impacto que producen las nuevas tecnologías en lo que respecta a la protección de los datos personales, cuando en especial, son tratados por terceros en entornos cloud.

Palabras clave: Tecnología. Datos personales. Privacidad. Terceros. Computación en la nube

Abstract

The provision of services such as cloud computing or cloud computing offers numerous economic and technical advantages for different organizations that decide on it and carry out its implementation. This thesis aims to take a look at the national laws and evaluate the impact that new technologies produce when it comes to the protection of personal data, when in particular, they are treated by third parties in cloud environments.

Key words: Technology. Personal information Privacy. Third parties Cloud computing.

Índice

Introducción General 6

Capítulo 1 Análisis del concepto de Datos Personales 15

Introducción 16

1.1 Diferencia entre datos e información 17

1.2- Concepto jurídico de datos personales 19

1.3 Derecho a la protección de datos personales 22

1.4- Transferencia internacional de datos personales. Alcance del concepto. 26

1.5- La llamada "cloud computing" o computación en la nube 31

1.6. Características esenciales de la "cloud computing" 33

1.6.1 Modelos de Prestación de servicios en "cloud computing" 35

1.6.2 Formas de despliegue de los servicios de "cloud computing" 36

Conclusión 38

Capítulo 2 Los datos personales en la Legislación Nacional 40

Introducción 41

2.1- El Habeas Data y su incorporación en la Constitución de la Nación Argentina . 44

2.2- El Habeas Data y los Tratados con Jerarquía Constitucional 48

a) Antecedentes extranjeros 51

b) Antecedentes Legislativos Nacionales. Ley 24745 "La Ley que no pudo ser" 52

2.4 Ley 25326 (Habeas Data) 52

2.5 Decreto Reglamentario Nº 1558/2001 54

2.6 Aspectos procesales de la Ley de Habeas Data 57

2.7 Código Civil y Comercial de la Nación 59

Conclusión 62

Capítulo 3 Análisis jurisprudencial del Habeas Data en la República Argentina . 64

Introducción 65

3.1 Jurisprudencia nacional sobre habeas data. Casos relevantes. 66

a) Fallo Urteaga, Facundo Raúl c. Estado Nacional - Estado Mayor Conjunto de las FF.AA. – s/amparo ley 16.986 66

b) Fallo R. P., R. D. c/ Estado Nacional – Secretaría de Inteligencia del Estado – 19/04/2011 68

c) Fallo Halabi, Ernesto c/ P.E.N. – ley 25.783 – dto. 1563/04 s/ amparo ley 16.986 ... 69

d) Fallo María Belén Rodríguez contra *Google Inc. s/* daños y perjuicios 72

3.2 Jurisprudencia extranjera 77

Conclusión 80

Capítulo 4 La Ley 25326. Su aplicación al tratamiento de datos personales por parte de terceros en entornos *cloud computing* 82

Introducción 83

4.1- Análisis de la transferencia internacional de datos personales 85

4.2- Ventajas y riesgos del almacenamiento de los datos personales en las llamadas "*cloud computing*" o computación en la nube 98

4.3- Cuestiones relevantes del almacenamiento de los datos personales en las llamadas *"cloud computing"* o computación en la nube 100

4.3.1 Aspectos jurídicos 100

4.3.2 Lista de verificación a la hora de contratar el servicio de *cloud computing* 101

Conclusión 103

Capítulo 5 El contrato de prestación de servicios tercerizados en entornos *cloud computing*..... 104

Introducción 105

5.1 El contrato de prestación de servicios de Cloud Computing 107

5.2 Consideraciones doctrinarias sobre el artículo 25 de la ley 25326 109

5.3 Características de los contratos *cloud computing* 113

5.4 Clausulas típicas de un contrato empresarial de servicios cloud computing 115

5.4.1 El contrato marco y sus anexos 115

5.4.2 Clausulas típicas 116

5. 5 La importancia de las cláusulas contractuales tipo de la Decisión 2010/87/UE 124

5.6 Perspectiva futura de las "cloud computing" 125

5.7 Consideraciones que podrían afectar la protección de los datos personales en ámbitos *cloud computing* 127

5.7.1 Datos personales encriptados o codificados 127

5.7.2 Datos personales fragmentados 129

5.7.3 Datos derivados o titularidad sobre los nuevos datos generados..... 129

5.8 Consideraciones acerca de la necesidad de modificación de la Ley Nº 25326... 131

Conclusión 133

Conclusión Final..... 134

Bibliografía..... 139

Introducción General

El hombre ha tratado siempre de usar herramientas y fuerzas para realizar sus trabajos o hacerlos más sencillos y rápidos. Fue así que surgieron las primeras computadoras electrónicas en la década de 1940, Colossus en Inglaterra y ENIAC en los Estados Unidos. Se trataba de máquinas calculadoras enormes, por ejemplo ENIAC, ocupaba una habitación de un tamaño considerable y generaba gran cantidad de calor.

Las computadoras fueron evolucionando de manera constante y vertiginosa, hasta convertirse en una herramienta indispensable para la vida actual. La mayor parte de los aparatos electrónicos están dotados de algún elemento de computación. Al respecto expresa Seymour Papert: "Hace sólo unos pocos años, la gente consideraba a las computadoras artefactos costosos y exóticos. Sus usos comerciales e industriales afectaban a la gente común, pero casi nadie suponía que habrían de convertirse en parte de la vida cotidiana. Esta perspectiva se ha modificado en forma vivida y rápida, a medida que el público llegaba a aceptar la realidad de la computadora personal, suficientemente pequeña y económica para ocupar un lugar en todo living o incluso en todo bolsillo" (Seymour Papert, 1981, pag.15).

"En torno a los años 70 y 80 se produjo una sinergia entre los campos de los computadores y las comunicaciones que ha desencadenado un cambio drástico en la tecnologías, productos y en las propias empresas que desde entonces, se dedican simultáneamente a los sectores de los computadores y de las comunicaciones…" (Stallings, 2000, pág. 4).

En la década de los 80 se vivió en el mundo una espectacular revolución de las comunicaciones a distancia con la aparición de las tecnologías que serían las bases de Internet, que se expandirían por todo el mundo. La infraestructura de Internet ha revolucionado las comunicaciones mundialmente a un nivel de importancia como lo fueron el telégrafo o el teléfono en el pasado. Es cuando aparece la llamada informatización de la sociedad, la cual sigue en ascenso, y actualmente nadie conoce o predice los niveles que puede llegar a alcanzar.

"Siempre ha sido difícil predecir qué tan rápido o dramáticamente una nueva tecnología transformará el mundo"[1]. Y con cada nueva tecnología, los efectos económicos, políticos y sociales se han sentido más rápido que nunca antes, expreso Bill Gates en un discurso pronunciado al cumplirse un aniversario más de la presentación de la primera computadora personal de escritorio.

Ya en las conclusiones de su libro "Ser Digital" Negroponte es optimista con respecto a la tecnología, pero no por ello deja de tener sentido común al prever que en el futuro habrá casos en que la propiedad intelectual será violada, nuestra privacidad invadida, habrá piratería de software y robo de datos.

Es así que en un primer momento, había temor por la posible intromisión del Estado en la vida privada con propósitos de seguimiento, y por su capacidad de centralizar toda clase de información relacionada a los ciudadanos. Lo que resulto ampliamente superado por el crecimiento de la tecnología informática en manos de empresas privadas, motivadas por sus propios incentivos económicos, al haberse incrementado enormemente la posibilidad técnica de manejar grandes volúmenes de información gracias a los recolectores de información que ya no encuentran límite ni fronteras al haberse desarrollado una técnica llamada *data-mining*.

Data Mining, también referenciado como Descubrimiento del Conocimiento en Bases de Datos (Knowledge Discovery in Databases o KDD), ha sido definida como el proceso de extracción no trivial de información implícita, previamente desconocida y potencialmente útil. También se puede decir que es una herramienta que ayuda a generar conocimiento para la toma de decisiones, descubriendo patrones de comportamiento o cualidades en los datos que se utilizan para predecir actitudes futuras.

Manifiesta Bill Gates en su libro Los negocios en la era digital: "Las eras económicas anteriores han venido definidas por largos períodos de estabilidad, seguidos de breves períodos de innovación que lanzaban a la crisis una serie de industrias. En una teoría evolucionista llamaríamos a este fenómeno un equilibrio intermitente. Hoy día las

[1] http://www.lanacion.com.ar/327043-los-primeros-20-anos-de-la-pc-segun-bill-gates

fuerzas de la información digital crean un entorno empresarial en constante cambio. En la misma teoría llamaríamos a esta situación un caos intermitente, es decir, una inestabilidad constante interrumpida solo por breves periodos de tranquilidad. A ratos el ritmo del cambio resulta inquietante en ocasiones.”

Como ha señalado Lorenzetti, entre otros, "Existe un nuevo espacio: el cibernético ("cyberespacio"), distinto del espacio físico, con una arquitectura caracterizada por su maleabilidad, puesto que cualquiera puede redefinir códigos e interactuar, lo que lo convierte en un objeto inasible y renuente a las reglas legales sobre jurisdicción." Pasó un tiempo desde que se escribieron estas líneas, en la actualidad el panorama es más complejo. También expresaba Lorenzetti que "existe una nueva temporalidad, que presenta como característica la simultaneidad, el "tiempo virtual", y la disolución de la distancia en la interacción inmediata, lo que plantea problemas legales como, por ejemplo, establecer si se trata de contratos entre presentes o ausentes, o compraventas a distancia". Continuaba relatando el citado autor que "existe una nueva noción de ciudadanos: los *netizens* que son "navegantes felices", pero socialmente cada vez más aislados y sin capacidad crítica. Ello nos pone frente a la necesidad de establecer cuáles son los derechos que estos ciudadanos tienen en la comunidad virtual."
Finalmente diagnosticaba que "semejante mudanza de los presupuestos hace pensar que lo mismo debería ocurrir en el Derecho, con nuevas herramientas y nuevos conceptos. Hasta la actualidad el fenómeno no se ha producido, puesto que el "*cyberlaw*" es examinado con las categorías conceptuales del derecho común, y sus conflictos son similares: regulación o flexibilidad, protección de la propiedad, del consumidor, de la privacidad. Las categorías analíticas y metodológicas proceden por analogía, y a pesar de que nos fascinan los nuevos términos, los examinamos mediante una asimilación a los fenómenos conocidos" (Lorenzetti, citado por Molina Quiroga, 2011).

El progreso tecnológico en materia de medios de captación de imagen y sonido (cámaras y grabadores diminutos –escondidos o disimulados dentro de otros objetos-, teléfonos celulares con sistemas de captación fotográfica, filmación y reproducción sonora, etc.) convierte a sus portadores en potenciales registradores de la intimidad de las personas. Se ha tornado imposible controlar el avance cuantitativo y cualitativo de estos instrumentos, incluido el uso de Internet, es necesario que el Estado –a través de

sus magistrados- pueda resguardar la privacidad de las personas, evitando que se vean sorprendidas por la curiosidad o el morbo de terceros. De lo contrario, no tardaremos en convertir a nuestra sociedad en un gran "panóptico"[2]. Sólo que aquí los presos no serían los que infringen la ley, sino los que son víctimas de una cierta concepción de progreso. (Rosatti, 2010)

Cuando Rosatti relaciona el tema con la obra "El panóptico" hace referencia a cómo somos observados mediante Internet, llegando a conocer nuestros gustos, aún los más íntimos y privados.

El jurista ingles Bentham desarrolló en la mencionada obra una teoría para que los presos pudieran ser vigilados por una o dos personas desde la torre de control y que, al estar bajo la mirada permanente del vigilante, bajaran sus umbrales de violencia, al extremo de no querer o no desear volver a delinquir.

El eje central de este sistema presidiario es la presencia continua de un ojo omnipresente en todo momento. Esta idea de presidio, ha sido reflejada de una u otra manera por muchos autores, por ejemplo George Orwell en 1984, critica a un sistema basado en un Gran hermano (*Big Brother*) que lo ve todo, y los ciudadanos en todo momento son controlados por éste. El Estado ejerce un control total sobre la vida y el pensamiento de sus ciudadanos. La libertad se reduce a la mínima expresión, y es algo que va poco más allá de pequeñas decisiones cotidianas sin ninguna trascendencia. Foucault, en "Vigilar y Castigar" habla de que la sociedad es un auténtico panóptico de Bentham, en la que los mecanismos disciplinarios tienden a salir de los ámbitos concretos en los que funcionaban para aparecer en todo el entramado social. En nuestros días se puede

[2] "El panóptico", es un modelo de prisión ideado por Jeremy Bentham. El mismo se basa en una construcción circular, de forma que, colocando una torre de vigilancia en medio, se podría vigilar a todos los presos a la vez con un mínimo consumo económico y personal. Lo peculiar de este sistema consiste en que la torre de guardia estaría tapada con celosías de forma tal que el que esté en su interior vería fuera mientras que los presos no sabrían si hay alguien vigilándoles o no. Este modelo se aplicó en muchas prisiones posteriores, como la Cárcel Modelo de Madrid, en la Cárcel de Caseros de Buenos Aires (Argentina) y en la Penitenciaría de Lima (Perú).

entender, como un sistema perverso que utiliza la evolución tecnológica, el uso de Internet y los medios de comunicación masivos, como medio de control social.
Se puede decir aunque parezca una ironía, que la sociedad moderna, converge en muchos puntos con las teorías de Bentham, Orwell o Foucault. Pues se observa que las redes sociales, los *smartphones*, y la hiperconectividad de la que somos partes, sientan las bases de un presente y un futuro con múltiples riesgos.

Es así que somos objeto de vigilancia a lo largo y ancho del planeta, ya no se limita a un edificio público o privado, con una cámara de seguridad, o a una intersección de avenidas importantes en una ciudad, sino que tenemos, permanentemente, el "ojo del poder", enfocado hacia nosotros. En muchas ocasiones sin contar con nuestra autorización expresa, tal vez sí tácita, en otras ni ésta, nuestra vida entera se registra en datos, imágenes y audio que se almacenan a grandes escalas, eso sí, controlada por unos pocos.

Así se llega a un hecho relevante en la actualidad, vinculado, justamente al uso, manejo y obtención de los datos personales por parte de los Gobiernos, grandes empresas o grandes corporaciones. ¿Se encuentran ellos autorizados? ¿A través de qué instrumentos? ¿La ciudadanía, el consumidor o quien los autorizó? ¿Qué objetivos tienen los gobiernos y las grandes corporaciones en la recolección de datos personales?

Entonces, ya transitando 2018, se puede decir que no hay vuelta atrás con respecto al avance de las telecomunicaciones y la informática. Hay que dictar normas para nosotros y nuestra posteridad, sabiendo que seguramente serán necesarias modificaciones o reemplazarse por otras en un futuro no tan lejano debido al avance incesante de las mismas.

Estamos ante un avance que no tiene parangón con otros hechos, por la rapidez de los cambios que no terminan de asimilarse cuando ya aparecen otros nuevos. Es así que actualmente se observa el surgimiento y gran uso de lo que se ha dado en llamar como *cloud computing* o computación en la nube que se la puede describir como un modo de externalización – *outsourcing* o tercerización– de servicios basada en Internet que lo pueden realizar individuos particulares, empresas, Estado y también distintos tipos de

organizaciones. Con este nuevo desarrollo de computación en la nube surgen muchos interrogantes jurídicos, todos ellos de gran relevancia y de gran complejidad. Motivo por el cual se me hace necesario delimitar el presente TFG a un tema en especial, que tiene que ver con la contratación de este nuevo modo de servicio, el cual será desarrollado en forma detallada en el último capítulo del presente trabajo.

Luego de haberse planteado el estado actual en que se encuentra la temática en estudio, se presenta como **problema del TFG** el siguiente:

"Analizar y determinar si la normativa vigente regula de manera adecuada y suficiente la protección de los datos personales cuando su tratamiento es realizado por terceros en entornos de computación en la nube."

Y su **objetivo general** es:

Analizar y determinar si las normas jurídicas vigentes en nuestro país regulan de manera adecuada y suficiente la protección de los datos personales cuando estos son almacenados y tratados por terceros en las llamadas "*cloud computing*" o computación en la nube.

Del objetivo general se derivan, entre otros, los siguientes objetivos específicos, para poder así alcanzar el objetivo general planteado:

- Explicar jurídicamente el significado de datos personales.

- Describir lo que se entiende por computación en la nube o *"cloud computing".*

- Definir lo que se entiende por transferencia internacional de datos personales.

- Analizar la Ley Nº 25326 - Protección de datos personales y su vinculación con los contratos de tercerización. El análisis se restringe a las relaciones B2B producto de la externalización de servicios de TI.

- Evaluar si es necesaria la modificación de la Ley 25326.

Así, ya en esta instancia se puede plantear como **hipótesis** del TFG la siguiente:

Este trabajo busca demostrar que la normativa legal vigente en nuestro país es insuficiente para una protección adecuada de los datos personales cuando se almacenan y tratan en entornos de *cloud computing* o computación en la nube.

Siendo su marco metodológico el siguiente:

El tipo de estudio que se utiliza en el presente trabajo es el **exploratorio.** Tiene como propósito principal examinar un problema de investigación que es novedoso, poco estudiado y del que se tienen muchas dudas y que puede dar inicio a nuevas investigaciones.

Por lo tanto es necesario recurrir al tipo **descriptivo**, el cual permite especificar propiedades, características, en definitiva hacer una descripción del fenómeno mediante la caracterización de sus rasgos generales.

Se analizan fuentes legales, doctrinarias y jurisprudenciales para obtener una idea cabal de la situación actual de la temática del trabajo a desarrollar.

Cabe mencionar que la computación en la nube es un tema novedoso, no solo a nivel nacional sino también internacional, motivo por el cual no hay suficiente doctrina al respecto.

En cuanto a la estrategia metodológica, se utiliza el **método cualitativo** el cual permite la comprensión de los hechos, comportamientos y procesos.

El punto de partida es la Constitución Nacional de 1994 y su implicancia en los derechos personalísimos de los ciudadanos. Las fuentes por lo tanto son las siguientes: doctrina, jurisprudencia, tratados internacionales, derecho comparado entre otras.

El TFG plantea en el **Capítulo 1**, una introducción general acerca de los conceptos de dato e información, para luego abordar jurídicamente el concepto de datos personales y de la intimidad.

A continuación, se presenta un tema medular esto es, lo referente a transferencia internacional de datos personales y lo que se entiende por Cloud Computing de acuerdo al Instituto Nacional de Estándares y Tecnología (NIST – *National Institute of Standards and Technology*) de los Estados Unidos y su laboratorio de tecnología de información.

Con lo que se estaría dando respuestas a los objetivos específicos 1- Explicar jurídicamente el significado de datos personales- y 2 -Describir lo que se entiende por computación en la nube o *"cloud computing"*-.

Para luego abordar en el **Capítulo 2**, la recepción de los datos personales en normas vigentes nacionales y en los Tratados Internacionales de jerarquía constitucional.

Al presentarse la normativa vigente en la Argentina sobre la protección de datos personales, se hace un breve repaso de cómo fue incorporado el habeas data en la reforma de nuestra Constitución en el año 1994 y luego la sanción de la Ley 25326. Lo cual nos servirá de fundamento para tener una idea completa de lo que los doctrinarios llaman "estado del arte" sobre el marco legal relativo a la protección de datos personales cuando los mismos son almacenados en las llamadas "*cloud computing*" o computación en la nube.

Con lo que se estaría contribuyendo a dar respuesta al objetivo general del presente trabajo.

En **Capítulo 3** se abordará la recepción del hábeas data después de la reforma de la Constitución de la Nación Argentina en el año 1994 y su aplicación jurisprudencial en fallos de gran relevancia. Estos fallos marcan el avance jurisprudencial en los temas vinculados a los datos personales, al derecho de la información y al gran progreso tecnológico. A la vez, como se convierten las nuevas tecnologías en objeto de estudio por parte de los juristas y doctrinarios por los desafíos que las mismas traen al derecho. También se consideran fallos de jurisprudencia extranjera por el impacto que tuvieron a nivel internacional.

En el **Capítulo 4** se hará un breve análisis de los artículos más relevantes de la Ley 25326 y que inciden de manera preponderante en el tratamiento de los datos personales

cuando los mismos son almacenados y tratados en las llamadas "*cloud computing*" o computación en la nube.

Se considerarán especialmente los siguientes artículos:

Artículo 9 - Seguridad de los datos.

Artículo 10 - Deber de confidencialidad.

Artículo 11- Cesión.

Artículo 12 -Transferencia internacional.

Artículo 25 -Prestación de servicios informatizados de datos personales.

Se pondrá el énfasis en la importancia que tiene el artículo 12 en lo que respecta a la transferencia internacional de datos como así también cuando los mismos son tratados por terceros, *outsourcing*, (artículo 25, inciso 1) que tiene una estrecha vinculación con el tema en tratamiento.

Con lo que se estaría dando respuestas al objetivo específico: 3 -Describir lo que se entiende por transferencia internacional de datos personales.

En el **Capítulo 5,** se aborda de manera puntual la protección de datos personales y su vinculación con los contratos de tercerización y esto también permite evaluar si es necesaria la modificación de la Ley 25326, es decir que se estaría dando respuestas a los objetivos específicos 4 y 5 - y al objetivo general del TFG.

Capítulo 1 Análisis del concepto de Datos Personales

Introducción

Es innegable que esta revolución basada en las tecnologías de la información, está modificando la base de la sociedad a un ritmo acelerado.

Este impacto, que se ha producido en la vida de las personas con la incorporación de nuevas herramientas, influye directamente en el derecho. Éste, entendido como un conjunto de normas jurídicas que surgen de necesidades sociales, de cambios que requieren ser tenidos en cuenta y por lo tanto plasmado en normas.

En concordancia con lo expresado, Ettore Giannantonio, sostuvo que "la difusión de la informática en todos los aspectos de la vida social, ha dado nacimiento a nuevas posibilidades, nuevos intereses pero también nuevos peligros, dando necesario nacimiento a una nueva disciplina jurídica…" (Ettore Giannantonio, citado por Altmark y Molina Quiroga, 2011, pág. 1041).

> La moderna tecnología en el área informática de que se vale tanto el Estado como los particulares para mejorar su actividad, en sus respectivos ámbitos, ha generado nuevos peligros y lesiones. Éstos se manifiestan ante la utilización indiscriminada de los datos personales para fines ilícitos o inmorales, la desprotección de los sujetos ante la posibilidad de ser objeto de decisiones adoptadas con base en el tratamiento de datos falsos o discriminatorios y la desnaturalización del fin para el cual fue recogida la información sobre las personas. Como agravante, las redes, principalmente la World Wide Web, proporciona a toda esa información un inconmensurable canal de salida. (Gils Carbó, 2001, pág. 5)

Se puede considerar que la tarea de almacenar datos no es peligrosa en sí misma, pero sí lo es cuando en esos archivos se almacenan datos pertenecientes a otros, consentido o no el proceso de guarda y recolección, y con ello se difunde a terceros una información que afecta la vida privada y otros valores sensibles de las personas. (Toro, R. y Olivera Roque, E. (2009) El "derecho al olvido", matices y recepción legislativa, doctrinaria y jurisprudencial en el derecho patrio. *Revista Abeledo Perrot Córdoba. Buenos Aires*. Nº 3 (mar-2009) 241-250)

Por todos estos cambios tan vertiginosos desde el punto de vista de la información y el uso que puede hacerse de ella, es que al decir de Altmark D. y Molina Quiroga, ha surgido por parte de los juristas la necesidad de realizar un análisis de la cuestión, especialmente en el tratamiento del dato personal. Es decir visualizar el tema del dato personal y su vinculación con el derecho a la intimidad y la problemática que surge por la estructuración de grandes bancos de datos de carácter personal y su impacto en la protección legal de esos datos.

1.1 Diferencia entre datos e información

Generalmente en las carreras afines a Sistemas, en primer año se aclara la diferencia entre dato e información. Un **dato** no es otra cosa que una representación simbólica de alguna situación o conocimiento, sin ningún sentido semántico, describiendo situaciones y hechos sin transmitir mensaje alguno. Puede ser un número, una letra, un signo ortográfico o una descripción. Entonces, los datos describen hechos empíricos de manera cruda, son tomados sin ser procesados y analizados.

Mientras que la **información** es cuando los datos son procesados y analizados, de modo que se pueda predecir o entender la realidad y puedan proveer un mensaje que contribuya a la toma de decisión para resolver un problema o incrementar el conocimiento en las personas que tienen acceso a dicha información.

Se puede definir a la Informática de acuerdo al diccionario de la RAE, como el "conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras".

Por consiguiente, un "Sistema Informático" se puede entender como la solución al planteo de un problema concreto de tratamiento automatizado de datos.

Se dice que vivimos en la "era del silicio" y es porque todos los electrodomésticos de nuestra casa, así como también ordenadores, móviles, mp3 y otros, contienen circuitos integrados o microprocesadores cuya materia prima es el silicio. En efecto, el material semiconductor del que están hechos los chips de las computadoras es tan importante para la sociedad actual como lo fue el carbón para la sociedad del siglo XIX.

Asimismo, resulta innegable que esta revolución basada en las tecnologías de la información, está modificando la sociedad toda a un ritmo acelerado. Es así que las economías de todo el mundo se han hecho interdependientes a escala global. Debido a que hoy en día están conectados a escala planetaria y cualquier turbulencia en un mercado es conocido e incide al instante en todo el mundo.

Manuel Castells (2005) en su obra "La era de la información – economía, sociedad y cultura-" expresa:

> Las redes convergen hacia una metarred de capital que integra los intereses capitalistas a escala global y a través de sectores y ámbitos de actividad: no sin conflicto, pero bajo la misma lógica abarcadora. El trabajo pierde su identidad colectiva, individualiza cada vez más sus capacidades, sus condiciones laborales, y sus intereses y proyectos. Quienes son los propietarios, quienes los productores, quienes los gestores y quienes los servidores se vuelve cada vez más difuso en un sistema de producción de geografía variable, de trabajo en equipo, de interconexión, de *outsourcing* y de subcontratación. ¿Cabría decir que los productores de valor son los brujos informáticos que inventan nuevos instrumentos financieros para ser desposeídos de su trabajo por los agentes de bolsa de las compañías? ¿Quién contribuye a la creación de valor en la industria electrónica: el diseñador de chips de Silicon Valley o la joven de la cadena de montaje de una fábrica del este asiático? Sin duda ambos, si bien en proporciones bastante diferentes. (p. 511)

Se puede afirmar que, al igual que la energía fue el motor de la Revolución Industrial, la información es el eje sobre el que gira esta revolución digital, en la que confluyen un

conjunto de tecnologías. Hoy podemos afirmar, que ya tenemos convergencia de tecnologías y que se avizora un futuro todavía más interesante para las TIC, seguramente más cambio en casi todos los aspectos de la vida.

Por lo expresado, es evidente que con cada desarrollo tecnológico viene aparejado un gran número de cambios que nos da ventajas y desventajas. Al haber mayor propagación de las TIC en nuestro país, habrá también mayores riesgos como ocurre en todo el mundo. Cuantas más cosas se realicen en internet, más información crítica de las personas y las empresas estarán alojadas en la Red. Los riesgos de ataques o de filtraciones, con consecuencias graves, son cada vez más altos.

Debiera ser política de Estado la inversión en seguridad en redes y en el encriptado de la información clasificada como sensible con métodos lo más seguros posibles y que minimicen la posibilidad de acceso a la misma, como así también la legislación que acompañe y brinde seguridad jurídica a los ciudadanos de la República.

1.2- Concepto jurídico de datos personales

En nuestro país la Ley Nº 25326[3] (Protección de Datos Personales – sancionada en octubre de 2000) y su Decreto reglamentario Nº 1558/2001[4], regulan la Protección de Datos Personales.

Además, el órgano de aplicación de la Ley de Protección de Datos Personales es la Dirección Nacional de Protección de Datos Personales (DNPDP), creada en el año 2001.

En el artículo 2[5] se dan las definiciones correspondientes:

[3] Ley 25326. Honorable Congreso de la Nación Argentina.

[4] Dec. 1558/2001. Reglamenta Ley de Protección de datos personales.

[5] Artículo 2, Ley 25326. Honorable Congreso de la Nación Argentina.

ARTÍCULO 2° — (Definiciones).

A los fines de la presente ley se entiende por:

— Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

— Datos sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

— Archivo, registro, base o banco de datos: Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

— Tratamiento de datos: Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

— Responsable de archivo, registro, base o banco de datos: Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.

— Datos informatizados: Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado.

— Titular de los datos: Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley.

— Usuario de datos: Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos.

— Disociación de datos: Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable.

Para dar el concepto jurídico de datos personales también se recurrirá a conceptos dados por doctrinarios de conocida trayectoria.

Para Molina Quiroga:

> La información es un concepto complejo, que se integra con "datos". El dato es el "antecedente necesario para llegar al conocimiento exacto de una cosa" y la información puede definirse como el proceso de adquisición de conocimientos que permiten precisar o ampliar los que ya se tenían sobre una realidad.
>
> Cuando el segmento de la realidad que es objeto de información es una persona, estamos frente a datos de carácter personal, con un alcance amplio, es decir que si de las operaciones de tratamiento posibles pueden establecerse relaciones referencias o asociaciones, con personas –sean éstas determinadas o determinables- deba considerarse a los datos involucradas como "datos de carácter personal", debiendo ser así tenidos en cuenta.
>
> En principio, se denominan datos personales aquellos que permitan identificar a la persona a la que pertenecen; en cambio, no se consideran tales los que se refieren a personas indeterminadas. El nombre y apellido es un dato personal (nominativo); la cantidad de personas de género femenino o masculino que concurren a un curso es un dato general.
>
> Dentro del género "datos personales" se denominan "sensibles" los referidos a determinadas facetas o aspectos de una persona, tales como el culto que profesa, su pertenencia racial, su ideología política, y en general la información que permite determinar su fisonomía moral e ideológica. La preocupación esencial que rodea el tratamiento de estos datos, además de la tutela del derecho a la

intimidad, o vida privada, es sin duda, la posibilidad de discriminación. (Molina Quiroga, 2011, p.483)

Hondius afirma que es "aquella parte de la legislación que protege el derecho fundamental de libertad, en particular el derecho individual a la intimidad respecto del procesamiento manual o automático de datos". Pérez Luño la define expresando que es "el conjunto de bienes o intereses que puedan ser afectados por la elaboración de informaciones referentes a personas identificadas o identificables". Estadella Yuste afirma que "se puede decir que el derecho a la protección de datos o a la autodeterminación informativa esta solapado con una parte importante del derecho individual a la intimidad; esta es la que hace referencia a la protección de los datos personales de la esfera privada". (Ekmekdjian – Pizzolo, 1995, p.6)

1.3 Derecho a la protección de datos personales

En nuestro país, la protección de los datos personales y su tratamiento están regulados por la Ley 25326.

Así, la Ley 25326 de Protección de los Datos Personales, sancionada en octubre del año 2000, y un poco más reciente nos encontramos con el nuevo Código Civil y Comercial –Ley 26994[6]–, que regulan los derechos vinculados a la titularidad y difusión de datos personales.

El llamado "nuevo" Código Civil y Comercial, incorpora un capítulo dedicado a los derechos personalísimos (Capítulo 3: Derechos y actos personalísimos).

Los llamados derechos personalísimos –también llamados "derechos esenciales de la persona" o "derechos fundamentales" – son aquellos que le corresponden a toda persona

[6] Ley 26994. Honorable Congreso de la Nación.

desde antes de su nacimiento y hasta la muerte, y que le garantizan el pleno desarrollo de su humanidad.

Justamente, la incorporación de varios artículos en el Código Civil y Comercial dedicados a los derechos personalísimos es uno de los puntos destacados de esta nueva normativa y que si los vinculamos a las nuevas tecnologías vemos como las normas van abarcando temáticas que no mencionaba de manera expresa el código anterior (vg. derecho a la imagen, o la captación de la imagen o la voz de una persona).

La inclusión de regulaciones respecto a la imagen, la dignidad y la difusión de informaciones personales, refleja la necesidad de establecer reglas de juego más claras para la vida pública y la circulación de datos personales en tiempos de Internet.

El capítulo de los derechos personalísimos protege al individuo frente a los progresos que ha tenido la globalización, la economía y la tecnología. Estas producen avasallamientos a los derechos individuales, intromisión a la privacidad, uso de imagen en sentido amplio, datos personales e intromisión médica.

Otra importante modificación es la incorporación de los contratos electrónicos, pero el código no hace una diferencia con los contratos informáticos, ni regula a estos últimos.

A continuación, también se recurrirá a puntos de vista dados por distintos doctrinarios respecto al derecho a la protección de datos personales.

Molina Quiroga (2011) afirma:

> El derecho a la "protección de datos" pertenece al contexto de la era informática, y cada día es más dudoso afirmar que esta compleja disciplina legal estuviera ya implícita en las referencias generales al derecho a la intimidad insertas en cuerpos normativos del ámbito nacional o internacional de la era preinformática.
>
> La fundamentación jurídica del derecho a la protección de datos personales debe relacionarse con el tradicional derecho a la intimidad, o a la vida privada, pero lo excede. (p.484)

Con respecto al derecho a la protección de datos, Germán Bidart Campos entiende que "los bienes jurídico protegidos son la intimidad, la zona de reserva personal, la

autodeterminación informativa, por lo que considera que se exigen controles eficaces. Y es la persona a la que pertenecen los datos que ingresan a un archivo o banco de datos, quien ha de poder verificar qué es lo que referente a ella se registra, de que fuentes y con cuáles procedimientos se obtiene, qué uso se le da, dentro de que límites es lícita la difusión y transmisión, y para qué fines" (Bidart Campos, citado por Puccinelli, 2004, prologo).

Por su parte Cifuentes (1978) describe a la vida privada como:

> El reducto intransferible de la soledad". Afirma que "en la soledad el hombre se agranda, interioriza, alimenta el vuelo de su espíritu; conserva el impulso de las fuerzas interiores; y también, se achica, toca lo bajo y palpa la sima de la propia miseria. En la soledad se comunica con lo sobrenatural, cultiva la inteligencia y el talento; el genio desborda en el campo propio de su expansión; el amor puede manifestarse con plenitud; los afectos entrañables crecen y florecen, se llora y se sufre; masivo y pobre ser aquel que, en alguna medida, no la busca ni la goza. (p. 336)

La tecnología de avanzada, la automatización, la comunicación electrónica, la multiplicidad de datos que recopila el sistema, son algunos de los aspectos que influyen para tomar muy en cuenta métodos de encriptación, bloqueos y, en definitiva, el derecho eventual a la reparación de daños. Reaparecen así, derechos y bienes jurídicos que demandan tutela, porque no es vano recordar que desde la Constitución y el derecho internacional de los derechos humanos hay que prestar lo que se denomina el acceso eficaz a la justicia. Tampoco es ajeno, en ciertas circunstancias, el concurso del derecho penal para incriminar y sancionar conductas.

Los derechos informáticos constitucionales precisan defensa, confidencialidad, preservación, discreción, vigilancia y control (Puccinelli, 2004).

Al decir de Gozaíni (2011):

> Las nuevas tecnologías de la información son un arma de doble filo: aumentan nuestras capacidades y nuestro poder, pero también hacen a sus usuarios más vulnerables a la vigilancia y a la manipulación. Ambos aspectos son

> inseparables: es precisamente lo que aumenta nuestras capacidades lo que nos hace más vulnerables. El ciberespacio no constituye una excepción: navegar por la red nos permite nuevas formas de comunicación con persona de todo el mundo, pero también puede significar que todas nuestras comunicaciones puedan ser interceptadas por terceros que, al mismo tiempo, nos localizan e identifican. Esto puede querer decir que otras personas o grupos están construyendo un perfil en red de nosotros mismos: qué direcciones visitamos, que anuncios nos interesan, que productos compramos, a que periódicos nos suscribimos o con quien mantenemos correspondencia electrónica. (p.10 y 11)

Por lo que se puede decir que la protección de los derechos fundamentales, y en especial el de la intimidad, puede verse afectada de una manera particular en el sector de las comunicaciones electrónicas. Si bien es cierto que en nuestro país, el derecho a la intimidad es atendido por normas como el artículo 18 y 19 de nuestra Constitución Nacional, se constató la necesidad de contar con algunas precisiones.

> "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", el primer párrafo del artículo 19 de la Constitución Nacional permite distinguir, dentro de las acciones humanas, un ámbito jurídico de otro que es irrelevante para el Derecho; en cuanto al segundo párrafo del artículo, en la medida en que establece que "Ningún habitante de la Nación será obligado a hacer lo que no manda la Ley, ni privado de lo que ella no prohíbe", permite distinguir –ahora dentro del mundo jurídico- lo permitido de lo prohibido (o antijurídico). (Rosatti, 2010, p. 287 y 288)

Recordando que: "Antes de toda regla positiva, la jurisprudencia ha establecido que el Internet es un nuevo medio de comunicación por el que se expresan actividades de todo orden (científicas, comerciales, periodísticas, personales) que está al amparo de la Constitución" (Molina Quiroga, 2011, p.612).

En relación al tema cabe recordar que en el año 2005 se sancionó y promulgó la ley Nº 26.032 que en su artículo 1° expresa: "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".

Por lo que se observa que habrá siempre una tensión permanente entre lo expresado anteriormente y la privacidad -la protección de datos personales-.

Más aún, se observa que la relación existente entre el derecho y la sociedad actual se da en un contexto de capitalismo y de una gran globalización y en una sociedad en extremo informatizada. Precisamente, la era de la información se basa en las comunicaciones y en las tecnologías de la información, ambas a grandes escalas. Por ende, se advierten nuevos problemas e interrogantes como los que se plantean en este trabajo de investigación, frente a los cuales el Derecho debe aportar soluciones específicas, si es que no las posee ya.

Por ello es necesario que los que hacen derecho en sus distintas esferas posean un adecuado conocimiento de la irrupción de las tecnologías de la información y sus implicancias, para poder así dar el abordaje de soluciones adecuadas y específicas a los interrogantes que se presentan. Entonces, es el Derecho, el que debe actualizarse y adaptarse a las nuevas realidades y requerimientos de la época, debiendo ser flexible pero no por ello sumiso en extremo. Porque se sabe ya, que Internet es un medio que vino para quedarse y va por mas, como así también se sabe, que no cambia sus normas ya existentes.

1.4- Transferencia internacional de datos personales. Alcance del concepto.

Justamente, Internet es una de las mayores revoluciones de la humanidad, para ella no hay barreras ni fronteras y con el avance incesante de la tecnología y las comunicaciones estamos en cualquier lugar del planeta en cuestión de minutos, lo que generó y genera un cambio irreversible en materia de comunicaciones, economía, cultura y en la sociedad toda, por lo que se la debe pensar como un fenómeno multidimensional. Por lo que resulta imposible separarla del uso que hacen las personas de ella, y por ende el impacto que tiene en nuestra sociedad. Entonces, surgen preguntas como:

> ¿Quién y Cómo se gobierna Internet? Siendo actualmente un recurso vital para la humanidad, es necesario entender quiénes y cómo se toman las decisiones que permiten que internet funcione correctamente, así como normas, estándares tecnológicos que regulan su uso y el contenido que fluye a través de sus nodos dispersos a lo largo y ancho del mundo y qué lugar ocupa dentro de este entramado la Protección de los Datos Personales y en general, de la Privacidad.
>
> Se puede decir que "Internet ha sido desarrollada de manera abierta e inclusiva desde el día 0, cuando sus creadores, distintos académicos y estudiantes de Universidades Norteamericanas fueron creando de manera colaborativa y democrática los estándares que dieron lugar a lo que hoy conocemos como la *World Wide Web*". (Altmark, 2015, p.149)

Es así, que el mencionado grupo de estudiantes y académicos fueron dándole cierto orden y estructura a la publicación y elección de estándares y así, conformaron lo que se dio en llamar el "Grupo de Trabajo en Red" o "*Network Working Group*".

Esta organización fue mutando hasta lo que actualmente se conoce como el "Grupo de Trabajo en la Ingeniería de Internet" o "*Internet Engineering Task Force* (IETF)", actualmente una de las organizaciones no gubernamentales más relevantes en lo que se refiere al mantenimiento y desarrollo de la gran infraestructura técnica de Internet como así también en la fijación de estándares tecnológicos. Los estándares son sólo reglas que definen como deben funcionar las cosas, permitiendo una uniformidad que es necesaria para que no haya problemas de compatibilidad. Razón por la cual el IETF está formado por gente que viene de proveedores de servicios, fabricantes de equipamiento, investigadores, profesores, estudiantes y otros, ya que básicamente, cualquier interesado puede participar.

Sabido es que el gobierno de los Estados Unidos siempre estuvo muy ligado al proceso de gestación de la red, de hecho financió gran parte de su desarrollo y luego se "apropió" en cierto modo, con el objetivo de proteger a la red de las posibles manipulaciones por parte de otros países, del Sistema de Nombre de Dominio o DNS. El DNS es lo que permite asignar a cada equipo un nombre y una dirección para que sea fácil de encontrar por cualquier usuario. En términos sencillos, es lo que permite

acceder a Google a través de www.google.com.ar en lugar de tener que recordar su dirección IP 216.58.216.238.

En la actualidad se utiliza el concepto de Gobernanza de Internet, para comprenderlo hay que remontarse a la Cumbre Mundial sobre la Sociedad de la Información (*World Summit on Information Society*, en adelante CMSI) en Ginebra en el 2003, donde se comenzó a trabajar mediante el Grupo de Trabajo sobre Gobernanza de Internet en una definición que surgió dos años después en el mismo encuentro en Túnez.

Se llegó a una definición sobre Gobernanza de Internet -aunque existen ciertas discrepancias en los términos utilizados- la cual es entendida de la siguiente manera: "La Gobernanza de Internet es el desarrollo y la aplicación por parte de los gobiernos, el sector privado y la sociedad civil, en sus respectivos roles, de principios, normas, reglas, procedimientos de toma de decisiones y programas comunes que dan forma a la evolución y utilización de Internet" (Altmark, 2015, p.150).

En el 2011, las Naciones Unidas[7] preparó un informe para que el Consejo Económico y Social comunicara a la Comisión de Ciencia y Tecnología para el Desarrollo acerca de los progresos, obstáculos y limitaciones realizados a nivel regional e internacional en lo que atañe a la Sociedad de la Información.

En uno de los puntos del informe, hace referencia a la privacidad y seguridad de los datos y explica lo siguiente:

A medida que aumentan el número de personas conectadas a Internet y el volumen de datos almacenados en los sistemas informáticos y los centros de datos lo hace también la inquietud por la privacidad y seguridad de los datos. El espionaje industrial y los riesgos para la seguridad nacional y la confidencialidad comercial preocupan a gobiernos y empresas. Preocupan a ciudadanos y organizaciones de la sociedad civil la explotación de los datos personales por organismos gubernamentales y empresas y el riesgo de ser víctimas de la suplantación de identidad y otros abusos fraudulentos.

[7] http://unctad.org/es/Docs/a66d64_sp.pdf

En otro punto del informe, este es el que más nos interesa, menciona la naciente "computación en nube" o “cloud computing” expresando que:

Otra innovación que puede tener consecuencias para la privacidad y la seguridad es la "computación en nube". Esta arquitectura alternativa de las TIC traslada tareas que hasta ahora se llevaban a cabo en el hardware y el software del usuario a aplicaciones, hardware y software que se encuentran en el ciberespacio.

Más adelante dice: Se prevé que la computación en nube tendrá gran efecto más allá del sector de la tecnología de la información, en el de la producción, como la manufactura, los medios de comunicación y la prestación de servicios públicos de salud y educación, entre otros. Su éxito puede depender en parte de la capacidad de las empresas de computación en nube y de los gobiernos y empresas poseedores de grandes bases de datos para disipar la preocupación por la privacidad y seguridad de los datos confidenciales almacenados en centros de datos y para replantearse las necesidades de seguridad de la gestión de los datos en este nuevo entorno digital.

En la mayoría de las veces hablar de Internet como así también de computación en la nube implica hablar de transmisiones internacionales. En esta primera instancia se recurrirá a enfoques dados por distintos doctrinarios para acercarse al concepto de ésta.

Al respecto expresa Palazzi (2002):

> El impresionante desarrollo de los últimos años en las autopistas de la información ha aproximado las distancias, borrado los límites territoriales y globalizados los negocios. Actualmente vivimos en un mundo de transmisiones internacionales de datos cotidianas. Cada vez que nos conectamos a Internet, cada vez que vemos un programa en televisión satelital, cada vez que compramos con tarjeta de crédito en el extranjero, o hacemos reservas para viajar en avión u hospedarnos en un hotel, lo más probable es que una transferencia internacional de información personal haya tenido lugar.
>
> La recopilación, la transferencia y el intercambio de datos personales acerca de individuos es cada vez más frecuente. Numerosos estudios se han encargado de demostrar como las tecnologías afectan la privacidad y como en especial la

> informática y las telecomunicaciones facilitan ampliamente la recogida de datos personales. Actualmente, internet, las autopistas de la información y los servicios online plantean también toda una serie de nuevos desafíos a la protección de datos personales. (p. 23 y 24)

Precisamente, "La convergencia de la informática y la telemática permite que la información sea transmitida sin restricciones de distancia, lo que conlleva a que los datos de un país desborden los límites del mismo e ingresen sin restricción alguna a otros países. El movimiento a través de las fronteras de datos e información para su tratamiento y almacenamiento en sistemas informáticos, genera innumerables inconvenientes y conflictos" (Masciotra, 2003, p. 357).

Sobre el tema expresa Mario Oyarzabal (2007):

> Un problema acuciante y relativamente novedoso que plantea el avance de la informática y de la tecnología de las telecomunicaciones se relaciona con el tráfico de datos personales, que incide sobre uno de los atributo más caros de la persona humana: *su derecho a la intimidad*, una de cuyas proyecciones consiste precisamente en "preservar en la confidencialidad y la reserva bienes personales como los que hacen al honor, la dignidad, la información 'sensible' [por ejemplo, la referida a orientación sexual, identidad étnica o racial, religión, ciertas enfermedades, e ideas políticas], la privacidad, la verdad, la autodeterminación informativa [y] la igualdad [que incluye el derecho a la identidad personal y el derecho a ser diferente]". (p.49 y 50)

Cuando los datos atraviesan una frontera y las diversas fases del tratamiento se realizan en territorios de Estados diferentes, es de prever el surgimiento de conflictos entre las leyes potencialmente aplicables a la controversia. Se pueden identificar cuatro tipos de leyes para la solución del conflicto:

a)- la ley del lugar de la sede del banco de datos,

b)- la ley del lugar de la sede o residencia del responsable del tratamiento,

c)- la ley personal del titular de los datos y,

d)- la ley del Estado donde tiene lugar la principal actividad del tratamiento.

La solución de esos conflictos corresponde, por esencia, al derecho internacional privado (Oyarzabal, 2007).

1.5- La llamada "cloud computing" o computación en la nube

Internet ha experimentado un crecimiento espectacular en estas últimas décadas y sigue creciendo más y más cada día. Es la base para múltiples aplicaciones tanto de ocio como de negocios y por ella circula información de lo más diversa. El número, tipo y variedad de servicios que se ofrecen a través de Internet es también cada día mayor. Es de público conocimiento que para Internet no hay barreras ni fronteras y con el avance incesante de la tecnología y las comunicaciones que se producen día a día estamos en cualquier lugar del planeta en cuestión de minutos y en la actualidad la utilización de este medio como vía de información y comunicación trae aparejado cambios sustanciales, tanto que podría afirmarse que supera en uso y preferencia a las redes telefónicas y en esta sociedad globalizada, compite con gran éxito en materia de información con la prensa oral y escrita.

Precisamente, la globalización ha traído aparejada la posibilidad de que otros modelos irrumpan en nuestra vida y convivan con nosotros, haciéndonos ganar algunas cosas y perder otras, como no podría ser de otra manera, existen ventajas y desventajas con este fenómeno. Otros símbolos patrios, otros idiomas, otras formas de hacer negocios, otras costumbres, otras canciones populares se ven y escuchan a diario en este mundo invadido por la convergencia de distintos medios de comunicación. Producciones extranjeras ocupan las programaciones en cine, televisión y otros; valorándose este hecho pues nos permite ampliar nuestro horizonte y poder comparar lo nacional con lo extranjero.

Y con respecto a la globalización expresa Diego P. Fernández Arroyo (2003): "Lo que es verdad es que la globalización versión cambio de milenio es un fenómeno cualitativa y cuantitativamente diferente a cualquiera que haya existido antes. Y esto

es así, fundamentalmente, por el impacto que tiene sobre la internacionalización el desarrollo impresionante de las tecnologías aplicadas a la producción en serie, a los transportes, a las comunicaciones y a la informática" (p. 60).

Es así que llegamos a que hoy en día se puede decir que las fronteras o límites nacionales son líneas dibujadas en los mapas como tampoco existen prácticamente husos horarios debido a que el flujo de negocios y comercio corre o correrá libremente en una economía global digitalizada sin fronteras y sin husos horarios.

También, durante estos últimos años surgió un concepto de gran importancia en lo que se refiere a la portabilidad, movilidad y convergencia tanto de hardware como de software que se conoce como "*cloud computing*", más conocido por su traducción al español como "computación en la nube". Esta nueva tendencia tecnológica es un concepto surgido de la necesidad de colocar o almacenar en servidores de Internet, dedicados a esta finalidad, las aplicaciones y documentos que el usuario utiliza para sus necesidades, con el objetivo de que pueda disponer de los mismos en el momento que los necesite y desde cualquier lugar de nuestro planeta, y siempre y cuando disponga de una conexión a Internet, es decir se encuentre "online" o "conectado".

Asimismo, comienza a causar preocupación en diferentes países el tema del almacenamiento de los datos personales de los ciudadanos en las nubes de internet llamadas "*cloud computing*", más precisamente el control y la transferencia internacional de los mismos. Entre las ventajas que presenta el almacenamiento de datos en la nube se puede mencionar: 1) la de cubrir las necesidades crecientes de almacenamiento masivo de información y al mismo tiempo reducir los costos; 2) almacenar y acceder a los datos desde diferentes dispositivos conectados a internet. Y entre desventajas que se pueden mencionar: 1) los riesgos de pérdida o violación de datos privados y confidenciales; 2) la gran cantidad de información almacenada por millones de usuarios hace que sean un blanco u objetivo atractivo para cualquiera que pretenden robar o acceder a información valiosa.

También, es evidente que con cada desarrollo tecnológico viene aparejado un gran número de cambios a favor y en contra. Al haber mayor propagación de las TIC en nuestro país, habrá también mayores riesgos como ocurre en todo el mundo. Cuantas

más cosas se realicen en internet, más información crítica de las personas y las empresas estarán alojadas en la Red. En un mundo en el que Internet se ha instalado cómodamente en nuestra vida cotidiana, la transferencia internacional de datos es un hecho inevitable que desafía las fronteras físicas y jurídicas de los Estados. Las fronteras físicas ya han sido derrotadas, es un hecho, mientras que las jurídicas subsisten en la norma y buscan su camino para establecer procedimientos razonables que garanticen la legitimidad del acto.

En los últimos años, gran cantidad de empresas se ven atraídas por las ventajas técnicas y los bajos costos de mantenimiento que ofrece el esquema de cómputo en la nube o *cloud computing*. Flexibilidad, accesibilidad, autoservicio bajo demanda, escalabilidad, gestión de grandes volúmenes de datos, son algunos de los beneficios que ofrece este esquema de cómputo.

El Instituto Nacional de Estándares y Tecnología (NIST – *National Institute of Standards and Technology*) de los Estados Unidos y su laboratorio de tecnología de información, define a *cloud computing* de la siguiente manera:

Cloud Computing es un modelo para habilitar acceso conveniente por demanda a un conjunto compartido de recursos computacionales configurables, por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios, que pueden ser rápidamente aprovisionados y liberados con un esfuerzo mínimo de administración o de interacción con el proveedor de servicios.

1.6. Características esenciales de la "*cloud computing*"

Este modelo de nube promueve la disponibilidad y está compuesto por cinco características esenciales, tres modelos de servicio y cuatro modelos de despliegue.

Las características esenciales son:

1) Autoservicio por demanda. Un consumidor puede abastecerse unilateralmente de capacidades computacionales, tales como tiempo de servidor y almacenamiento en red,

de acuerdo a sus necesidades y de forma automática sin requerir de una interacción humana con cada proveedor de servicio.

2) Amplio acceso a la red. Las capacidades están disponibles a través de la red y se acceden a ellas a través de dispositivos estándar (por ejemplo, teléfonos móviles, laptops, tabletas).

3) Reservas de recursos en común. Los recursos computacionales del proveedor (como por ejemplo el almacenamiento, el procesamiento o la memoria) se agrupan para servir a múltiples clientes usando un modelo de arriendo múltiple, con diferentes recursos físicos y virtuales, que son asignados dinámicamente y reasignados en función de la demanda de los consumidores. Existe un sentido de independencia de la localización en que el cliente por lo general no tiene control o conocimiento de la localización exacta de los recursos provistos. Usualmente el proveedor no revela el lugar, aunque se puede especificar una ubicación o localización a un nivel más alto de abstracción genérica, como por ejemplo la región, país o *datacenter*. Ejemplo de estos recursos incluyen almacenamiento, procesadores, memoria, ancho de banda, máquinas virtuales entre otros.

4) Rapidez y elasticidad. Las capacidades pueden suministrarse de manera rápida y elástica, en algunos casos de manera automática, para poder escalar rápidamente y ser liberadas rápidamente para reducir la escala de operación. Para el consumidor, las capacidades disponibles para abastecerse a menudo parecen como ilimitadas y pueden ser adquiridas en cualquier cantidad y en cualquier momento.

5) Servicio supervisado. Los sistemas en nube automáticamente controlan y optimizan el uso de los recursos utilizando una capacidad de evaluación en algún nivel de abstracción adecuado para el tipo de servicio (p.ej., almacenamiento usado, procesamiento, ancho de banda, y cuentas de usuario activas). El uso de recursos puede ser monitoreado, controlado y reportado, proveyendo transparencia para ambos, el proveedor y el consumidor del servicio utilizado.

1.6.1 Modelos de Prestación de servicios en "cloud computing"

Existen tres diferentes modelos de prestación de los servicios en la nube y se definen del siguiente modo:

1) Infraestructura como Servicio (IaaS- del inglés *Infrastructure as a Service*) En este modelo de infraestructura como servicio, el *Cloud Service Provider* (CSP) brinda al usuario una infraestructura de recursos, la cual incluye procesamiento, energía, almacenamiento, redes y otros recursos fundamentales de computación para que el consumidor pueda implementar y ejecutar cualquier tipo de aplicación. También suele llamárselo *Hardware as a Service*. Aquí, el usuario tiene control sobre los sistemas operativos, almacenamiento, aplicaciones desplegadas. Este esquema puede escalarse automáticamente, según las necesidades del cliente. Un ejemplo de proveedor del modelo IaaS es Amazon y con su *Elastic Compute Cloud* (Amazon EC2).

2) Software como Servicio (SaaS – *Software as a Service*) En *Software* como servicio, la capacidad que se le promociona al consumidor consiste en utilizar las aplicaciones del proveedor que se ejecutan en una infraestructura de nube, las cuales pueden accederse desde distintos dispositivos e interfaces del cliente (p.ej., correo, web, VPN). En este nivel, el consumidor no administra ni controla la infraestructura de nube subyacente en la que se basa el servicio que utiliza. El rango de aplicaciones de un SaaS comprende: servidores de correo electrónico, editores de documentos, redes sociales, almacenamiento, etc. Exponente del modelo SaaS es *Google Drive*. Se trata de un producto de Google que reemplaza a *Google Docs* que permite almacenar, crear, modificar, compartir y acceder a documentos, archivos y carpetas de todo tipo en un único lugar. Una de las ventajas de esta aplicación es que no están ligada a una PC específica; no es necesario descargar ni instalar ninguna aplicación en una computadora en particular, y cualquier dispositivo con acceso a internet puede acceder también a las aplicaciones que brinda *Google Drive*. Debido a que cada usuario guarda la información en la nube, puede acceder a dicha información desde cualquier punto. También permite la concurrencia de usuarios para editar los mismos archivos al mismo tiempo, lo que permite encarar procesos de colaboración online. En este servicio, el usuario accede a

aplicaciones que se ejecutan directamente sobre la infraestructura y la plataforma del proveedor.

3) Plataforma como Servicio (PaaS - Platform as a Service) En la plataforma como servicio, en cambio, la capacidad proporcionada al consumidor es el despliegue de todo lo necesario para la construcción y puesta en marcha de aplicaciones y servicios web completamente accesibles en Internet. El consumidor no administra ni controla la capa de infraestructura de la nube pero gestiona las aplicaciones allí instaladas junto con la posibilidad de controlar su entorno y configuración. En ocasiones, los proveedores de PaaS suministran las herramientas de desarrollo necesarias para la plataforma. Un claro ejemplo de PaaS es *Google App Engine* (GAE). Se trata de una plataforma gratuita que ofrece Google desde el año 2008 que permite a los usuarios desarrollar, ejecutar y alojar sus aplicaciones web en la infraestructura de Google. El modelo de desarrollo de aplicaciones que ofrece dentro de GAE permite el crear aplicaciones en leguaje *Pyton y Java*, administrarlas vía una interfaz web y publicar la aplicación en los servidores de Google. Otros ejemplos entre otros de proveedores y productos PaaS son: *Oracle Cloud Platform for Data Management y Red Hat OpenShift.*

1.6.2 Formas de despliegue de los servicios de "cloud computing"

Independientemente del modelo de servicio utilizado (SaaS, PaaS, IaaS) y teniendo en cuenta la titularidad de las infraestructuras en la nube, existen cuatro formas de despliegue de los servicios de *cloud computing*:

1) Nube Pública: la infraestructura de la nube está disponible para el público en general a través de internet. En este despliegue los clientes contratan los recursos que necesiten para sus proyectos, siendo el proveedor del servicio el responsable del mantenimiento y de la gestión de la infraestructura, lo que reduce significativamente los costos iníciales de desarrollo, de estructura y acceso inmediato a sus servicios en contratación.

2) Nube Privada: la infraestructura de la nube se provisiona para el uso exclusivo de una única organización con múltiples usuarios (áreas de negocio, departamentos, etc.). La característica principal de este modelo de despliegue es que el usuario no comparte

infraestructura física con ningún otro cliente, agrupando los servicios y la infraestructura en una red privada, lo que ofrece un mayor nivel de seguridad y control. Se basa en la reserva de recursos de *hardware y software* en exclusiva para un usuario.

3) Nube comunitaria: la infraestructura de esta nube es compartida por varias organizaciones de una comunidad específica que comparten intereses similares (p.ej., misión, requisitos de seguridad, políticas, jurisdicción y consideraciones sobre cumplimiento normativo). Puede ser gestionada y operada por una o más de las organizaciones involucradas, por terceros o una combinación de ambos.

4) Nube Hibrida: El cliente gestiona exclusivamente su infraestructura, pero dispone de acceso a los recursos de la nube pública que controla el CSP en sus instalaciones, pudiendo ampliar sus recursos en cualquier momento, obteniéndolos de la nube pública.

Entonces, se observa que muchos interrogantes se plantean con el tema del almacenamiento de los datos personales de los ciudadanos en las llamadas *Cloud Computing* o cómputo en la nube. Por ejemplo qué tribunales pueden entender en un conflicto generado en la nube y que protección se garantiza tanto a los ciudadanos como a los países intervinientes.

Debiera ser política de Estado la inversión en seguridad en redes y en el encriptado de la información clasificada como sensible con métodos lo más seguros posibles y que minimicen la posibilidad de acceso a la misma, como así también la legislación que acompañe y brinde seguridad jurídica a los ciudadanos de la República.

Conclusión

Es sabido que la Ciencia y la Tecnología se retroalimentan mutuamente. Se puede definir a la Ciencia de acuerdo al diccionario de la RAE[8], como el "Conjunto de conocimientos obtenidos mediante la observación y el razonamiento, sistemáticamente estructurados y de los que se deducen principios y leyes generales con capacidad predictiva y comprobables experimentalmente".

Mientras que se puede definir a la Tecnología de acuerdo al diccionario de la RAE, como el "Conjunto de teorías y de técnicas que permiten el aprovechamiento práctico del conocimiento científico".

En la actualidad, el mundo se encuentra guiado por el desarrollo de las ciencias y de las tecnologías, las cuales se alimentan recíprocamente. Está claro que los problemas más urticantes surgen en la tecnología. Aquí, la conciencia puede jugar un rol fundamental ya que se puede impedir la falacia del "imperativo tecnológico" según el cual si una cosa es posible entonces es buena, a la luz de la distinción aristotélica entre hacer técnico, cuyo fin es el *bonum operis*, la perfección de la obra, y el obrar ético, cuyo fin es el *bonum operantis*, el bien del hombre. Porque no todo lo que es técnicamente posible es éticamente lícito. El "hacer bien" no es siempre "hacer el bien" y en caso de colisión entre las exigencias del arte, de la tecnología con las exigencias de la moral, considero que el arte, la tecnología deberían ceder ante los derechos de la moral ya que el fin último del hombre es "hacer el bien". Por lo que se puede decir que se trata de una obligación negativa, debido a que la moral se le impone al artista –ingeniero, técnico- como un valor que no se puede ceder, como un límite. Seguramente, en muchas ocasiones después de grandes luchas internas porque conviven en él, el hombre y el artista – ingeniero, técnico-, debido a que, para el desarrollo de la obra entran en juego todas las facultades humanas; es el hombre en cuanto hombre. Por ejemplo, expresan los que saben que la oda lirica de Bécquer o García Lorca nace en el fondo del ser, levanta y sacude ideas y decisiones, dudas y creencias, odios y amores, nostalgias, temores y rebeldías.

[8] Diccionario de la Real Academia Española. http://dle.rae.es

Es así, que, en este Capítulo 1 se trata de explicar la realidad tecnológica de nuestros días, instancia que considero previa y necesaria para abordar en el Capítulo 2 la legislación vigente en nuestro país sobre la temática abordada y así, dejar abierto el camino para más adelante evaluar y sugerir si es necesario implementar modificaciones a la normativa vigente en nuestro país con respecto a la protección de datos personales.

Capítulo 2 Los datos personales en la Legislación Nacional

Introducción

En este capítulo 2 se abordará la legislación vigente en nuestro país con respecto a la protección de los datos personales, con lo cual se pretende hacer un breve recorrido de cómo se ha llegado al estado actual de la misma. Cuestión que se considera fundamental para abordar en los capítulos 4 y 5 el estudio en mayor profundidad de la Ley 25326 y en especial el tratamiento de datos personales por terceros en entornos *"cloud computing"* o computación en la nube. Y recién ahí decidir si es necesaria su modificación por la aparición de estas nuevas formas de tratamiento y almacenamiento.

Así, la protección de los datos de carácter personal de los individuos y su vinculación con la tutela de los derechos a la identidad e intimidad, ha sido una preocupación de los juristas. Principalmente porque ese derecho a la intimidad consiste en mantener inviolada la propia esfera de la vida íntima, en una sociedad como la que marca la tecnología en la cual todo se vuelve objeto de información. De allí que originariamente ese derecho se formulara como derecho *to be let alone* (derecho de estar a solas).

Si este derecho a la privacidad nació bajo esa matriz, por fuerza debe cobrar inédita significación a medida que la invasión se hace cada vez más intolerable, a lo que se suma la aparición de los ordenadores e Internet en el campo de la informática y telecomunicaciones, circunstancia que viene a plantear la exigencia de reconocer un nuevo derecho a las personas.

Una cuestión importante a esclarecer es sobre los derechos que el hábeas data protege y de qué forma lo hace.
En nuestro Derecho[9], un sector de la doctrina lo ha asociado al derecho a la intimidad.
Así, Bidart Campos relacionó la indefensión de la persona frente al mal uso de sus datos y a la publicidad de los mismos con el derecho constitucional a la privacidad.
Expresa el autor: "No hay duda de que el objeto tutelado coincide globalmente con la intimidad o privacidad de la persona, ya que todos los datos a ella referidos que no

[9]Se tendrá en cuenta el artículo "El hábeas data en el derecho argentino" de P. Palazzi, Alfa-Redi Revista de Derecho Informático (No. 004 - Noviembre del 1998)

tienen como destino la publicidad, o la información a terceros, necesitan preservarse" (Bidart Campos, 1997, p.301).

Y más adelante agrega "La protección a los datos personales es imprescindible actualmente, y se vincula con un múltiple engranaje. El desarrollo tecnológico; el tratamiento electrónico de la información; los derechos de quienes acumulan datos en los registros y los de quienes quedan registrados; el flujo cibernético, etc., han hecho necesario compatibilizar "los valores fundamentales del respeto a la vida privada y de la libre circulación de la información", como reza el Convenio de Estrasburgo para los estados que son miembros del Consejo de Europa" (Bidart Campos, 1997, p.302).

Algunos autores lo consideran como un derecho humano de tercera generación que surge frente a la necesidad de una protección adecuada de la privacidad ante el avance desproporcionado de las tecnologías de la información.[10]

Otros, lo consideran una garantía al derecho a la intimidad[11], otros como una subespecie de amparo[12] y consideran que el propósito de su tutela consiste en evitar que el uso de la informática pueda lesionar tal derecho como así también el derecho al honor[13], otros ponen el énfasis en el riesgo que implica para la persona ya sea la estructuración de grandes bancos de carácter personal y la potencialidad de entrecruzamiento de la información contenida en los mismos.[14]

Cabe aclarar que otro sector de la doctrina prefirió relacionarlo con el derecho a la identidad[15] en sentido amplio o desde la identidad cultural del individuo.[16] El bien tutelado va a ser el patrimonio cultural, político, ideológico, religioso y social de la persona.

[10] Bergel citado por P. Palazzi en el artículo "El hábeas data en el derecho argentino".

[11] Ekmekdjian citado por P. Palazzi en el artículo "El hábeas data en el derecho argentino".

[12] Sagüés citado por P. Palazzi en el artículo "El hábeas data en el derecho argentino".

[13] Badeni citado por P. Palazzi en el artículo "El hábeas data en el derecho argentino".

[14] Altmark y Molina Quiroga citado por P. Palazzi en el artículo "El hábeas data en el derecho argentino".

[15] Guastavino citado por P. Palazzi en el artículo "El hábeas data en el derecho argentino".

[16] Cifuentes citado por P. Palazzi en el artículo "El hábeas data en el derecho argentino".

De lo expuesto surge que el habeas data protege un conjunto "complejo de derechos personalísimos", que incluyen la privacidad y la identidad, relacionados a su vez con la imagen y con los conceptos de verdad e igualdad.
Por lo tanto, esta realidad cultural, social que se transita en la actualidad, sumada al avance de la informática y las telecomunicaciones, torna razonable consagrar un derecho especial que proteja a las personas y les otorgue facultades para controlar las informaciones que de ellas consta en los archivos y bancos o bases de datos.

El habeas data puede ser considerado como un derecho garantía complejo. Cuando se habla acerca de su complejidad esto quiere decir que se lo toma de manera amplia. Es decir que tiene una intensa relación con el derecho a la integridad, a la dignidad humana, a la identidad, al honor, a la propia imagen, a la seguridad, a peticionar, a la igualdad, a la privacidad, no menos que la libertad de conciencia, a la libertad de expresión, a comerciar y con cualquier otro que, de cualquier forma, pudiera resultar afectado.

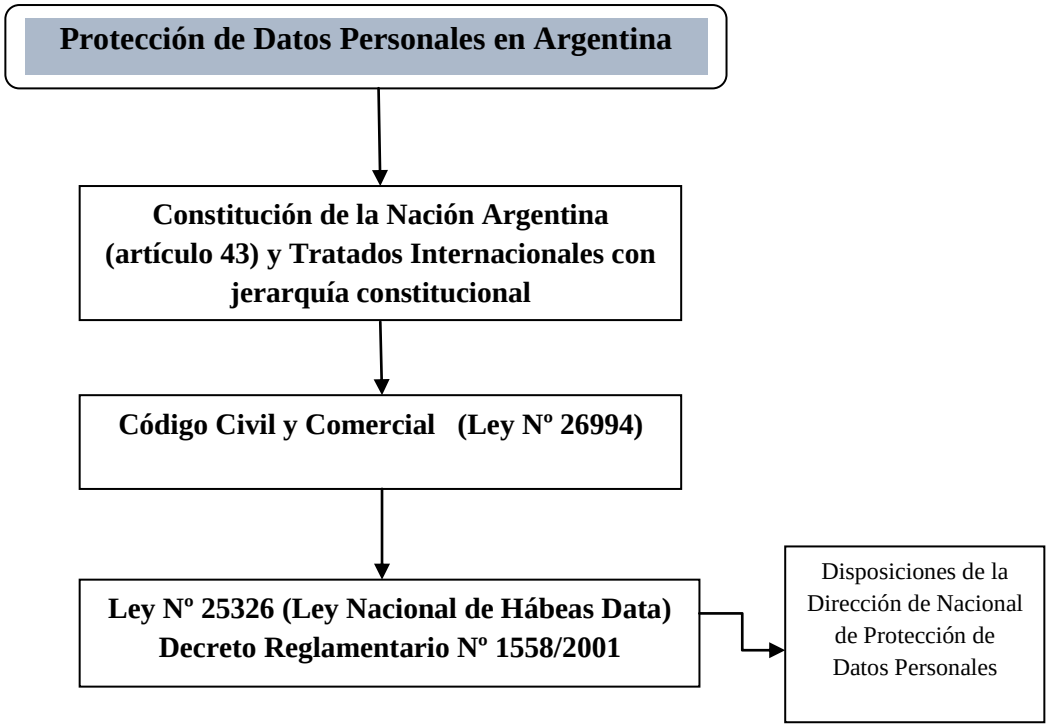
Por lo tanto, esas informaciones que hacen a circunstancias o condiciones personales deben ser protegidas de su divulgación y restringidas de su inclusión en archivos o bases de datos, a través de la tutela legal.

Por ello se va a analizar la protección de datos personales desde el reconocimiento de este derecho garantía en nuestra Constitución Nacional, para luego abordar el tema plasmado en los Tratados Internacionales y en el Código Civil y Comercial de la Nación, como así también en la Ley 25326 y en su Decreto Reglamentario.

Normativa Vigente en el país

Dentro del plexo normativo nacional contamos con las siguientes normas que se ven vinculadas al tema de datos personales:

En el siguiente cuadro se observa la normativa vigente en nuestro país.



2.1- El Habeas Data y su incorporación en la Constitución de la Nación Argentina

El instituto del *Habeas Data* es una de las garantías constitucionales más modernas, aunque se la denomine mitad en latín y mitad en inglés. En efecto, su nombre se ha tomado parcialmente del antiguo instituto del *Habeas Corpus*, en el cual el primer vocablo significa "conserva o guarda tu" y del inglés "*data*" sustantivo plural que significa "información o datos". En síntesis si se hace una traducción literal es "conserva o guarda tus datos".

Se puede afirmar siguiendo a Manili que "El origen de esta garantía puede situarse aproximadamente en 1968, año en que se realizó la Conferencia Internacional de Derechos Humanos de Teherán. La importancia que ésta reviste, está dada en que es a partir de ese momento en que los Estados advierten con claridad, el riesgo que implican

los avances tecnológicos y científicos –producidos por la revolución informática- en cuanto a la posible afectación a derechos humanos básicos; en el caso, el derecho a la intimidad"(Manili, 2010, p. 2).

A continuación, se va a transitar, como es que la convención reformadora de 1994, considera la necesidad de incorporarla a nuestra carta magna. La ley declarativa de la necesidad de reforma constitucional incluyó entre los temas habilitados para su enmienda, la consagración expresa del habeas corpus y el amparo, ignoró toda mención explícita a la expresión hábeas data. Sin embargo en el seno de la Convención, los temas fueron virando desde la protección de la libertad personal hasta el control de la actividad desarrollada por otros operadores de datos, cuyos registros respondan a finalidades publicitarias, comerciales o financieras y a las eventuales interferencias en la vida privada de las personas, que esa actividad pudiera generar (Gelli M., 2003).

Si tomamos la intervención de los convencionales Juan Pablo Cafiero y Delich, dentro de la Convención Constituyente muestran claramente este desplazamiento o ampliación de las garantías constitucionales: "…en un principio, la preocupación por incorporar la garantía del hábeas data a la Constitución Nacional, giro en torno a la necesidad de proteger a las personas frente al contenido de los registros y asientos que de ellas pudieran efectuar los organismos de seguridad del Estado…", por otro lado y desde la perspectiva de las garantías personales Delich manifestaba "…el ciudadano de la sociedad tecnológica desarrollada, brinda diariamente información sobre sus datos personales en múltiples formas y presiente que existen los medios para que toda su persona: su patrimonio, su formación escolar y universitaria, sus operaciones financieras, su trayectoria profesional, sus hábitos sexuales y su vida, sus esparcimientos, sus preferencias, su historia clínica, o sus propias creencias religiosas o políticas se hallen exhaustivamente registradas en archivos susceptibles de ser utilizados indebidamente…" (Boletín Nº 27, p. 1373).[17]

Por su parte, Quiroga Lavié, convencional en 1994, coincide en que el poder constituyente ha protegido con el articulo 43 el derecho a la intimidad con el sentido

[17] Para un análisis detallado de los debates, ver Masciotra, Mario. El hábeas data. La garantía polifuncional.

tuitivo definido por la Corte Suprema en el caso Ponzetti de Balbin que se configura como el "derecho a decidir por sí mismo en qué medio compartirá con los demás sus pensamientos, sus sentimientos y los hechos de su vida personal" (Rossatti, Barra, García Lema, Masnatta, Mosset Iturraspe, Paixao, Quiroga Lavié, 1994, p.157).

Lo que hizo el constituyente argentino no es otra cosa que proteger la intimidad con el sentido tuitivo definido por la propia Corte Suprema cuando ha sostenido que ella (la intimidad) configura "derecho a decidir por sí mismo en que medio compartirá con los demás sus pensamientos, sus sentimientos y los hechos de su vida personal".[18]

Si bien el Habeas Data, antes de la reforma de 1994, se desprendía del artículo 33 de la Constitución Nacional, el nuevo artículo 43 en su párrafo tercero lo incorpora expresamente al texto constitucional.

Así, el Hábeas Data en la Constitución Nacional quedó definido en el Art. 43 tercer párrafo: "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 habeas data puede ser tomado como un amparo especial ya que tiene una especificidad propia y no es una acción subsidiaria de otras. Además, por la peculiaridad de su finalidad, no requiere que quien haya registrado los datos y los transfiera o someta a alguna forma de tratamiento, haya obrado con arbitrariedad o ilegalidad manifiesta. Basta, por ejemplo, con que el dato sea erróneo y se transmita con negligencia para que la acción quede expedita (Gelli, 2003).

Si se asocia a cada una de las garantías del articulo 43 con los distintos estadios del constitucionalismo, se deduce que el hábeas corpus nace para el resguardo de la libertad corporal como un instrumento propio de la primera generación de derechos individuales reconocidos por la Constitución de 1853, el amparo –creado en forma pretoriana por la Corte en los casos "Siri" y "Koft"- fue una respuesta a los derechos

[18] C.S.J.N. "Ponzetti de Balbín c/ Editorial Atlántida S.A.", Fallos, 306:1892 (1984)

humanos de segunda generación. En este devenir, y frente a los avances de la informática y la genética, aparecen derechos de tercera generación, tutelados por el hábeas data (Verdaguer, 2010).

De todo ello se desprende que el hábeas data, junto con el amparo y el hábeas corpus, integran las tres garantías constitucionales por excelencia que aseguran a todo ciudadano -o mejor dicho, a cualquier habitante- el cese de la violación o amenaza del derecho constitucional conculcado.

Así, de la protección y seguridad de las personas, afectadas por datos erróneos o falsos asentados en registros públicos, la nueva institución pudo contemplar el resguardo de derechos tales como la intimidad, la imagen, el buen nombre y fama comercial, la identidad personal y familiar a través de la regulación de un amparo especial –el habeas data- denominado nuevo derecho en algunas de las intervenciones de los convencionales constituyentes. En efecto, la determinación de los lindes del hábeas data implica ejercicio y distribución del poder. Exige, por ello, la intervención del Estado como árbitro entre intereses y contendientes desiguales –los operadores de bancos de datos y los titulares de datos –pues, "la protección de datos personales constituye un importante criterio de legitimidad política de los sistemas democráticos tecnológicamente desarrollados".

> Allí donde se establezcan bancos de datos, cualquiera sea su carácter, no puede someterse a la persona humana a quedar enteramente expuesta y transparente por la acumulación de informaciones relativas incluso a su vida privada. La esfera de la intimidad vuelve el punto al origen de la vida; la necesidad de estar en soledad para saber que aun necesitando de los demás, relacionándonos con ellos, viviendo en necesaria e imprescindible comunidad, dando a otros nuestra cooperación y solidaridad, sirviendo en la vida y para la vida, aun con todo, es preciso ser uno, y definir en la reserva de nuestros sentimientos cómo queremos ser sin que nos invadan con datos y registros acerca de cómo se debe ser (Gozaíni, 2010, p.11).

2.2- El Habeas Data y los Tratados con Jerarquía Constitucional

La reforma de la Constitución Nacional de 1994, estableció la jerarquía constitucional de los tratados de derechos humanos, en su artículo 75 inciso 22, entre otros a la Declaración Universal de Derechos Humanos y a la Convención Americana sobre Derechos Humanos. Lo que significa que tienen jerarquía superior a las leyes dictadas por el Congreso de la Nación – supralegalidad – y también están en el mismo plano que la Constitución Nacional.

Los Estados ratifican o adhieren a los tratados y sus protocolos facultativos de forma voluntaria, entonces asumen la obligación jurídica de aplicar sus disposiciones y de informar periódicamente al órgano establecido en el respectivo tratado.

Los mencionados tratados de derechos humanos, son tratados destinados a obligar a los Estados parte a cumplir dentro de sus jurisdicciones internas, los derechos que los mismos tratados reconocen directamente a los hombres que forman parte de la población de tales Estados.

El compromiso y la responsabilidad internacionales, proyectan un deber "hacia dentro" de los Estados, el cual es el ya señalado de respetar en cada ámbito interno los derechos de las personas sujetas a la jurisdicción del Estado-parte firmante.

Al respecto expresa Sagüés "El mismo inciso añade que tales instrumentos tienen nivel constitucional "en las condiciones de su vigencia, tienen jerarquía constitucional, no derogan articulo alguno de la Primera Parte de esta Constitución y deben entenderse complementarios de los derechos y garantías por ella reconocidos" (Sagüés, 2007, p. 167).

"En definitiva, esos documentos no se encuentran solamente sobre las leyes, como cualquier tratado; también están en el mismo plano que la Constitución, aunque estrictamente, desde el punto de vista formal, no se inserten en ella" (Sagüés, 2007, p. 167 y 168).

Así también, en el pensar de Bidart Campos, "estos instrumentos no forman parte del texto de nuestra Constitución Nacional sino que se encuentran fuera de ella, pero a su

mismo nivel, lo que implica que comparten supremacía jerárquica por sobre el derecho infraconstitucional, conformando un "Bloque de Constitucionalidad Federal" (Bidart Campos, 1998, t. 1 p.337)

Cabe mencionar que existen normas sobre Derechos Humanos vinculadas al instituto de Habeas Data a saber:

a) La Declaración Universal de Derechos Humanos

b) Convención Americana sobre Derechos Humanos llamada Pacto de San José de Costa Rica

- Declaración Universal de Derechos Humanos

Artículo 12. – 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.

Este artículo 12 establece el derecho a la intimidad, a la honra y a la reputación. Este derecho debe estar garantizado respecto de todas esas injerencias y ataques, provengan de las autoridades estatales o de personas físicas o jurídicas. Además, cualquier intromisión en los asuntos mencionados realizada de forma ilegal supone una agresión a estos derechos y es denunciable ante los tribunales.

Artículo 19. – Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión.

Este artículo 19 resulta fundamental, ya que establece las tres facultades básicas en las cuales se divide el derecho a la información, derecho que le corresponde a todo individuo como derecho natural de la persona, que son las facultades de 1) investigar, 2) recibir y 3) difundir información.

- Convención Americana sobre Derechos Humanos llamada Pacto de San José de Costa Rica

Artículo 11. Protección de la Honra y de la Dignidad

1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. 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. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques. Expresa Feldman que:

> El derecho a la intimidad o privacidad que conlleva la imposibilidad de injerencias no solo de las demás personas sino del Estado. Por esto no son permitidas la interceptación telefónica o la filmación de escenas familiares, e incluye el derecho a la imagen y, en general, a la vida privada. La dignidad de la persona exige que su vida privada sea respetada y por eso violan este derecho quienes divulgan aspectos privados o familiares o atacan la honra sin ninguna consideración por el daño concreto o potencial que pudiera producir (Feldman, 2008 p. 47).

Artículo 25. Protección Judicial**.**

1. Toda persona tiene derecho a un recurso sencillo y rápido o a cualquier otro recurso efectivo ante los jueces o tribunales competentes, que la ampare contra actos que violen sus derechos fundamentales reconocidos por la Constitución, la ley o la presente Convención, aun cuando tal violación sea cometida por personas que actúen en ejercicio de sus funciones oficiales…

La norma emplea los vocablos “recurso sencillo y rápido” y luego agrega “efectivo”, lo cual está indicando que es necesario modificar muchas legislaciones en las que el hábeas corpus o amparo se prolonga en forma excesiva desvirtuando la finalidad y sentido de dicha institución. La reforma constitucional argentina receptó estos

principios consagrando explícitamente el hábeas corpus, el amparo y el hábeas data, este último a su vez limitado por el derecho o reserva de las fuentes periodísticas.

En conclusión, la incorporación de los tratados sobre derechos humanos en la Constitución Nacional ha cobrado particular importancia en lo que respecta a los derechos personalísimos como son los derechos que el habeas data recepta.

Por un lado hace un reconocimiento explícito a través de la Constitución y por el otro gracias al reconocimiento de estos tratados pone de relieve la uniformidad de las soluciones frente a problemas que no conocen de fronteras y que angustian al hombre. Es decir que los derechos fundamentales y las libertades que la constitución ampara, se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias. Además, es un instrumento para la defensa de los derechos humanos en el sentido de su consagración plena y de defensa en el supuesto de agresión o amenaza de agresión.

2.3- Antecedentes de la Ley Nº 25326.

a) Antecedentes extranjeros

Nuestro sistema regulatorio se inspira en el modelo europeo, que a través de su Directiva de Protección de Datos Personales 95/46/EC –sienta el principio general en materia de transferencia internacional de datos– y el actual Reglamento General 2016/769 establece una regulación integral sobre todos los sectores involucrados en el tratamiento de datos personales. En este sentido, el sistema regulatorio europeo se diferencia del sistema norteamericano, en éste la regulación se realiza por sectores y entonces, no existe una legislación general sobre protección de datos.

> La Exposición de Motivos de la Ley Orgánica Española del 29 de octubre de 1992 sobre Tratamiento Automatizado de Datos (LORTAD) dice que la "privacidad" es más amplia que la "intimidad", porque esta última se refiere a la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona, vgr. el domicilio donde realiza su vida cotidiana o las

> comunicaciones en las que expresa sus sentimientos, mientras que, la privacidad, constituye un conjunto más amplio y global de facetas de la personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado (Gils Carbó, 2001, p. 7).

b) Antecedentes Legislativos Nacionales. Ley 24745 "La Ley que no pudo ser"

El Congreso Nacional en 1996 sanciona la Ley 24745, llamada Ley de Habeas data. Esta Ley había tenido su origen en la Cámara de Senadores, a través de esta Ley se desarrollaba el artículo 43 CN.

Esta Ley fue aprobada después de fuertes discusiones en las cámaras, sin embargo luego de mucha polémica la Ley fue vetada por el presidente Menem.

Las causas del veto presidencial fueron las presiones de empresas transnacionales y consultoras de riesgo crediticio.

La Ley 24745, seguía los lineamientos de la Ley Orgánica de Regulación del Tratamiento de Datos de carácter Personal (LORTAD), vigente en España desde 1992 hasta la promulgación de la Ley Orgánica de Protección de Datos (LOPD) en 1999.

2.4 Ley 25326 (Habeas Data)

Como se ha analizado en puntos anteriores, el Hábeas Data en la Constitución Nacional quedó definido en el Art. 43 tercer párrafo, y luego de haber transcurrido más de seis años de la reforma de la Constitución, se dictó la ley 25326 de Protección de Datos Personales. Por lo que el Art. 43 tercer párrafo se encuentra regulado por la mencionada ley, la que enuncia en su Art. 1°: "protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos 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…"

La ley se divide en capítulos:

El primero habla de las disposiciones generales en el que se enuncia el objeto (artículo 1) y las disposiciones referentes a las definiciones necesarias para mejorar la interpretación de la ley (artículo 2).

El capítulo segundo cuando hace referencia a los principios relativos a la protección de datos indica los principios de licitud y de calidad de los datos. Es decir que los datos deben ser ciertos, exactos, concretos, pertinentes, actualizados y no excesivos.

El principio de la lealtad en la recolección, de la especificación del fin o de la finalidad, de la restricción de uso que está íntimamente relacionada con la finalidad. Además del principio de la limitación del tiempo, que consagra el derecho de olvido. La confidencialidad, el tratamiento de datos sensibles y la garantía de seguridad, la cesión y la transferencia internacional serán otros de los principios que van a tutelar los bienes jurídicos que la norma ampara.

Mientras que el capítulo tercero hace referencia a los principios relativos a los derechos de los titulares de datos.

A su vez en el capítulo cuarto trata los artículos referentes a usuarios y responsables de archivos, registros y bancos de datos. Es en este capítulo se encuentra el artículo 25, al cual se prestará mayor atención y estudio en el último capítulo por la relevancia que presenta para el tema en estudio en el presente TFG.

Estos cuatro capítulos, de acuerdo a lo que la misma Ley expresa son de orden público y todo lo que ello implica a nivel jurídico.

En el capítulo quinto se ocupa la ley del órgano de control de la presente normativa y de los códigos de conducta.

Mientras que en el capítulo sexto se trata el tema de las sanciones administrativas y penales.

En el capítulo séptimo se establece el marco legal de cómo se lleva a cabo propiamente la acción de protección de los datos personales.

Al decir de Sagüés, el Hábeas Data persigue una serie de "objetivos precisos" que el accionante sepa:

- Por qué motivos legales, el poseedor de la información llegó a ser tenedor de la misma.
- Desde cuándo tiene la información.

- Qué uso ha dado a esa información y qué hará con ella en el futuro.
- Conocer a qué personas naturales o jurídicas, el poseedor de la información le hizo llegar dicha información. Por qué motivo, con qué propósito y la fecha en la que circuló la información.
- Qué tecnología usa para almacenar la información.
- Qué seguridades ofrece el tenedor de la información para precautelar que la misma no sea usada indebidamente.
- Que información se tiene respecto a determinada persona y para qué se almacena.
- Si la información es actualizada y correcta y, de no serlo, solicitar y obtener la actualización o rectificación de la misma.
- Conociendo los datos, se supriman si no corresponde el almacenamiento, por la finalidad del registro o por el tipo de información de que se trata.
- En relación con los archivos o registros pueden ser tanto públicos como privados destinados a dar informe, así también van a ser tutelados: el honor, la intimidad y la autodeterminación informativa.

Su finalidad, entonces, consiste en proteger al individuo contra la invasión a su intimidad, su privacidad y honor, a conocer, rectificar, suprimir y prohibir la divulgación de determinados datos, especialmente los sensibles, evitando, pues, calificaciones discriminatorias o erróneas que puedan perjudicarlo.

2.5 Decreto Reglamentario Nº 1558/2001

Debido al avance de las nuevas tecnologías y a la influencia de la informática, nuestra Ley Nº 25326 viene a reconocer el derecho a acceder a la información almacenada por terceros en bases, registros, archivos o bancos de datos, públicos o privados referidos a cualquier ciudadano y a la facultad de actuar en consecuencia.

Al año siguiente de la sanción de la mencionada ley, el Poder Ejecutivo Nacional dictó el 3 de diciembre de 2001 su reglamentación a través del Decreto N° 1558/2001, con

el cual se completa y se vuelve operativo el círculo de protección en cuanto a este derecho personalísimo.

Entre los aspectos positivos del Decreto se pueden mencionar:

- Aclara el alcance de la Ley 25326, al establecer que se entenderá que: "quedan comprendidos en el concepto de archivos, registros, bases o bancos de datos privados destinados a dar informes, aquellos que exceden el uso exclusivamente personal y los que tienen como finalidad la cesión o transferencia de datos personales, independientemente de que la circulación del informe o la información producida sea a título oneroso o gratuito".

- Otro aspecto es el relativo a las transferencias internacionales ya que el decreto explica que tanto el consentimiento, como el uso de los datos provenientes de registros públicos son situaciones que permiten transferir el dato personal más allá de las fronteras (art. 12, Dec. 1558/01).

- La Ley 25326 no explica a que se considera *nivel adecuado de protección* a los fines de transferir datos personales (art. 12, de la Ley 25326), en cambio el decreto sí lo precisa, y establece que: "se entiende que un Estado u organismo internacional proporciona un nivel adecuado de protección cuando dicha tutela se deriva directamente del ordenamiento jurídico vigente, o de sistemas de autorregulación, o del amparo que establezcan las cláusulas contractuales que prevean la protección de datos personales" (art. 12, Dec. 1558/01).

- El decreto reglamentario trata de facilitar el ejercicio de los derechos reconocidos en la ley, para lo cual encomienda a la Dirección Nacional de Protección de Datos Personales la elaboración de modelos de formularios que faciliten el derecho de acceso de los interesados (art. 15, Dec. 1558/01).

- El articulo 21 expresa que deben inscribirse todos los bancos mencionados en el art. 1 del decreto reglamentario (art. 21, Dec.

1558/01), con lo que se aclara sobre cuál es el alcance de la ley y qué bancos deben inscribirse.

- El artículo 25 establece que "Los contratos de prestación de servicios de tratamiento de datos personales deberán contener los niveles de seguridad previstos en la Ley Nº 25326, esta reglamentación y las normas complementarias que dicte la Dirección Nacional de Protección de Datos Personales, como así también las obligaciones que surgen para los locatarios en orden a la confidencialidad y reserva que deben mantener sobre la información obtenida".

  Además, establece expresamente que: "La realización de tratamientos por encargo deberá estar regulada por un contrato que vincule al encargado del tratamiento con el responsable o usuario del tratamiento".

- El decreto reglamenta la constitución del Organismo de contralor, la aprobación de los códigos de conducta y el procedimiento de imposición de sanciones (arts. 29 a 31, Dec. 1558/01).

Para concluir se puede afirmar que al hablar del órgano de contralor, se tiene casi las mismas potestades que la Ley española otorga a la Agencia de Protección de Datos de España, con la independencia y autonomía un poco más acotada que la de España pero no por eso menos efectiva.

Entonces, comenzamos a ser vistos, por el resto del mundo, como uno de los primeros países latinoamericanos que consagrábamos constitucional, legislativa y reglamentariamente, la facultad otorgada a toda persona de controlar la información a ella referida, contenida en registros públicos y privados.

Así, después de este desarrollo legislativo, Argentina fue declarada país adecuado por la Unión Europea en materia de Protección de Datos Personales, de acuerdo a la "Directiva 95/46/EC". Nuestro país fue uno de los cinco primeros países, por fuera de la Unión Europea, en obtener este reconocimiento en el año 2003. Lo cual significa que se reconoce a la Argentina como país en condiciones de cumplir con los controles que

exige la Unión Europea y garantiza la debida salvaguarda o tutela de los datos personales.

El mencionado reconocimiento para Argentina constituye un beneficio significativo por diversas razones. En primer lugar, permite el libre flujo de datos y también elimina requisitos, autorizaciones y garantías adicionales para la transferencia internacional de datos personales. Esto a su vez impacta en un mayor grado de inversión en el país, ya que empresas de diversos rubros –tales como empresas de informática, financieras, call centers, etc.– contemplan a la Argentina con mayores ventajas comparativas respecto al resto de los países de la región.

2.6 Aspectos procesales de la Ley de Habeas Data

La Ley de Protección de los Datos Personales Nº 25326, en su Capítulo VII confiere marco legal a la "acción de protección de los datos personales o de hábeas data", regulación ésta que no es aplicable en la jurisdicción provincial, sino exclusivamente en el fuero federal y en el ámbito nacional. De conformidad a lo dispuesto en el art. 37 (Procedimiento aplicable), el procedimiento de la acción de hábeas data, debe ajustarse a las normas previstas en los arts. 38 a 43 de aquélla y en los aspectos no contemplados por las mismas se aplicarán las disposiciones contenidas en la Ley 16986 (Acción de amparo) y supletoriamente el art. 498 del C.P.C.C.N., que determina las reglas del proceso sumarísimo.

Legitimación activa: El art. 43 de la Constitución Nacional habilita el hábeas data a favor de "toda persona" (física o ideal), pero acto seguido especifica que lo es "para tomar conocimiento de los datos a ella referidos", entonces restringe la legitimación al afectado.

La ley 25326 otorgo también legitimación activa a los sucesores de las personas físicas, sean en línea directa o colateral, hasta segundo grado, art. 34, declarando que puede actuar también el defensor del pueblo, en forma coadyuvante (Sagüés, 2007).

Legitimación pasiva: la tienen los "registros o bancos de datos públicos, o los privados destinados a proveer informes" (art. 43 de la Const. Nacional). Quedan fuera de este proceso, los archivos de mero uso personal.

El art. 35 de la ley 25326 amplió la legitimación pasiva respecto de los usuarios de dichos bancos de datos, y el decreto 1558/01 permite atacar por el hábeas data a cualquiera de éstos, cuando exceda el uso exclusivamente personal.

En rigor de verdad, puede entenderse que este proceso constitucional también protege cualquier derecho constitucional perjudicado por un archivo o banco de datos. En tal sentido, el art. 1 de la ley 25326 amplió también la cobertura del hábeas data para garantizar el derecho al honor y a la intimidad de las personas (Sagüés, 2007).

> La dimensión que la Corte le ha dado al habeas data viene de algún modo a superar la visión que coloca a esta garantía sólo como un medio de verificar la falsedad o desactualización de un dato. En este punto, si bien existe un genuino interés privado en la difusión y transmisión de datos comerciales y también un interés del Estado en el registro de datos por razones de seguridad, creemos que el grave problema se presenta en la evaluación y relación de esa información, pues –como señala la profesora Gelli– aun cuando esa operatoria "no incluya datos sensibles de las personas, entraña mayor peligro para éstas, pues implica *opinión* traducida en el modo en que se califican aquellos datos". La tensión entre estos derechos debe ser cuidadosamente ponderada toda vez que el usuario es la parte más débil en la relación con las entidades crediticias y financieras que se valen de las bases de datos (Verdaguer, 2010, p. 483 y 484).

Así, "los oferentes cada vez que logran personalizar más sus productos captan información (muchas veces sin conocimiento del consumidor) en violación de los derechos de privacidad, a fin de personalizar aún más sus servicios y fidelizar y cautivar así a sus clientes. En suma, los beneficios arrojados por la personalización de los servicios de "*marketing on-line*", debe ser balanceada con los potenciales perjuicios que pueden surgir en referencia a la privacidad de los consumidores" (Rosatti, 2010, p.305).

Legitimación colectiva: la posibilidad de promover una acción de protección de datos personales de manera colectiva no está contemplada en la Ley 25326 sin embargo, se ha admitido su utilización desde la doctrina como desde la jurisprudencia.

A nivel jurisprudencial se amplió la legitimación a una asociación de usuarios y consumidores para promover la acción de habeas data colectiva. Además se ha entendido que la sentencia dictada en el marco de una acción de habeas data colectiva tiene efectos de cosa juzgada erga omnes, ya sea ésta condenatoria o absolutoria.

2.7 Código Civil y Comercial de la Nación

La protección de la dignidad de la persona humana, como objeto de tutela del habeas data, no estaba expresamente consagrada en el Código Civil ya que no contenía una enumeración de los derechos personalísimos. Todos los entes con signos característicos de humanidad, sin distinción de cualidades o accidentes eran considerados personas de existencia visible. Fueron la doctrina y la jurisprudencia las que brindaron las bases para su protección fundada en las normas presentes en la Constitución Nacional y en los tratados internacionales.

La nueva normativa del Código Civil y Comercial, en sintonía con la Constitución Nacional y los tratados internacionales firmados por la República Argentina, coloca a la persona humana, al sujeto en un estado donde su consideración tiene un valor intrínseco absoluto.

Antes, la afectación arbitraria de la intimidad personal estaba protegida dentro del marco del abuso del derecho. Se establecía la reparación en equidad. La intimidad familiar no era mencionada. La honra o reputación estaba protegida dentro de los hechos producidos por la fuerza y el temor. El Código civil computa las consecuencias resarcitorias de injurias o calumnias de cualquier especie y de una acusación calumniosa. La imagen de la persona no estaba legislada dentro del Código Civil, sino en la Ley 11723 (Régimen legal de la propiedad intelectual).

En cambio, en el nuevo Código Civil y Comercial[19], se considera la afectación de su intimidad como un atentado a su dignidad, por lo que habilita la prevención y reparación de los daños sufridos a este respecto. Remite a lo normado respecto de la responsabilidad civil que establece que la reparación integral por violación de los derechos personalísimos de la víctima, de su integridad personal, su salud psicofísica, sus afecciones espirituales legítimas y las que resultan de la interferencia en su proyecto de vida. La reparación del daño debe ser plena o sea la restitución de la situación del damnificado al estado anterior al hecho dañoso, sea por el pago en dinero o en especie. Expresamente prevé que en el caso de daños derivados de la lesión del honor, la intimidad o la identidad personal, el juez a pedido de parte puede ordenar la publicación de la sentencia o en sus partes pertinentes, a costa del responsable.

Está legitimado para reclamar la indemnización de las consecuencias no patrimoniales el damnificado directo y según las circunstancias, los ascendientes, los descendientes, el cónyuge y quienes convivían con aquel recibiendo trato familiar ostensible. Se incorpora la categoría de intimidad familiar como ámbito colectivo de autonomía. El factor de imputación es subjetivo.

Como así también la normativa del código civil no preveía la protección de la imagen o la voz de una persona. Su protección estaba referida en la Ley de Propiedad Intelectual, específicamente, en el art. 31 de la ley 11723.

Con posterioridad la doctrina y la jurisprudencia sostuvieron consistentemente la tutela del derecho a la propia imagen. Así, en el nuevo Código Civil y Comercial[20] se

[19] Conf. Artículo 52 CCyC Afectaciones a la dignidad. La persona humana lesionada en su intimidad personal o familiar, honra o reputación, imagen o identidad, o que de cualquier modo resulte menoscabada en su dignidad personal, puede reclamar la prevención y reparación de los daños sufridos, conforme a lo dispuesto en el Libro Tercero, Título V, Capítulo 1.

[20]Conf. Artículo 53 CCyC.- Derecho a la imagen. Para captar o reproducir la imagen o la voz de una persona, de cualquier modo que se haga, es necesario su consentimiento, excepto en los siguientes casos:
a) que la persona participe en actos públicos;
b) que exista un interés científico, cultural o educacional prioritario, y se tomen las precauciones suficientes para evitar un daño innecesario;
c) que se trate del ejercicio regular del derecho de informar sobre acontecimientos de interés general.
En caso de personas fallecidas pueden prestar el consentimiento sus herederos o el designado por el

establece que el derecho a la imagen y a la propia voz como un derecho personalísimo. La reproducción de la persona en su individualidad particular debe ser realizada con el consentimiento de ésta. De esto se desprende que la difusión que fue consentida para un fin no puede ser utilizada para otra finalidad sin que medie un nuevo consentimiento de la persona. Se puede concluir que ni la imagen ni la voz de una persona pueden utilizarse de modo que implique la espectacularización de la persona sin su consentimiento.

El código civil y comercial regula novedosamente a los contratos electrónicos dejando de lado la incorporación de los contratos informáticos.

Se denominan "contratos informáticos a los procesos negociales que tienen por objeto la prestación de bienes y servicios vinculados a la información automatizada" (Altmark, 2006. p.10).

A través del artículo 1105 se incorporan los medios modernos de comunicación en función de la contratación a distancia definiéndose cuales son estos tipos de contratos, por su parte el artículo 1106 establece una equiparación entre el tradicional instrumento contractual en soporte papel con el contenido en un soporte electrónico u otra tecnología similar, mientras el artículo 1107 brinda directivas sobre la celebración de un contrato de consumo a distancia realizado mediante medios electrónicos o similares, manteniendo la obligación de información a cargo del proveedor y los alcances de ella.

Tal como se puede apreciar, se han dejado algunas lagunas en lo referente a los contratos informáticos (empresas contratantes entre sí).

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.

Conclusión

En las sociedades informatizadas del presente, el poder ya no reposa sobre el ejercicio de la fuerza física, sino sobre el uso de información que permite influir y controlar la conducta de los ciudadanos, casi sin necesidad de recurrir a medios coactivos. Por ello, la libertad personal y las posibilidades reales de intervenir en los procesos sociales, económicos o políticos se hallan determinados por el acceso a la información. Tomar conciencia de esta situación significa reconocer, que en la coyuntura política actual la aceptación o no del orden social y jurídico por parte de los ciudadanos depende del correcto planteamiento que pueda hacerse de problemas tales como la protección de datos personales, del ambiente o de la manipulación genética.

La era tecnológica coloco al individuo de nuestro tiempo frente a la tecnología, en la misma disyuntiva que la era moderna encontró a los revolucionarios franceses frente al antiguo régimen. Es decir que la tecnología produce transformaciones en el plano político, jurídico, social y económico de los países.

Por ello, corresponde destacar, como mérito de los convencionales de la Convención Nacional Constituyente de 1994, el haber tenido la sensibilidad necesaria para introducir la problemática de la protección de los datos personales a la nueva Constitución.

Pasaron casi seis años desde el reconocimiento constitucional, para que se apruebe la Ley de protección de Datos y luego el decreto reglamentario. Fue un avance de la legislación argentina en ese momento.

Sabido es que el derecho no va a la par de las tecnologías porque estas cambian día a día, ya pasaron 17 años desde la promulgación de la Ley 25326 y se observa la aparición de nuevos problemas que la Ley no prevé, por lo que es conveniente que sea *aggiornada* a los tiempos que corren.

En conclusión, al analizarse la normativa vinculada a la protección de datos personales, se observa que no se menciona el tema de computación en la nube. Un tema que está muy en boga en nuestros días. Tanta importancia ha adquirido que en julio de 2017 el

gobierno argentino firmó un convenio de entendimiento con la empresa Amazon con el fin de que ésta brinde apoyo a empresas insipientes y además de brindar capacitación a docentes y alumnos para computación en la nube.

Por lo cual se puede concluir que aún sin normativa interna que lo contemple, ya está entre nosotros y lo más preocupante es que surgen dudas acerca de si se es dueño o no de nuestros archivos personales, laborales o programas en tanto están alojados en un disco duro de un tercero, en algún lugar del mundo, bajo legislación de no se sabe con exactitud de qué país. Por lo que se torna necesario, el aseguramiento por vía contractual de las mayores protecciones posibles para los datos personales, estos resguardos contractuales deben cubrir, como mínimo, los requerimientos normativos aplicables al cliente de *cloud computing* en función del objeto de su negocio, de su lugar de establecimiento, o de los procesamientos concretos que pretenda realizar mediante los servicios *cloud*. No obstante, se puede decir que en muchas ocasiones el cumplimiento normativo no implica necesariamente la protección efectiva de la información contra las amenazas en el ciberespacio.

Ya finalizando, se puede decir que la privacidad de millones de usuarios en el mundo es entregada a corporaciones a cambio de que hagan más simple y económico el acceso, el almacenamiento y el tratamiento de datos personales, es algo peligroso porque tendríamos que plantearnos si esto no es una acción más de entregar la soberanía del país.

Capítulo 3 Análisis jurisprudencial del Habeas Data en la República Argentina

Introducción

Se ha realizado, en capítulos anteriores, un análisis minucioso sobre el Derecho de Protección de Datos personales.

La doctrina no es pacífica, en cuanto al alcance de la aplicación de la Ley de protección de datos personales en ciertas cuestiones, por ejemplo, el IP *address*, (protocolo de internet) ¿es un dato personal?, otro problema que se presenta es que las normas atienden más al tema de la transmisión del dato personal que al tema de la recepción, se controla más a quien los envía, que a quien los recibe.

Si bien la Ley busca proteger los derechos del individuo frente a las nuevas tecnologías, que utilizan información personal, no es uniforme la aplicación de la normativa jurídica, ello se debe en gran medida a que las tecnologías de la información, superan ampliamente en velocidad a la respuesta que el derecho puede dar y también porque la naturaleza "digital" de estos temas hace que ciertos conceptos jurídicos clásicos quedan un poco desdibujados y seguramente necesitan una reorientación. Por ello, es que la protección de la intimidad, en particular, puede verse afectada por la expansión de Internet en todos los aspectos de la vida cotidiana y que ello ha representado en general un reto para el derecho en sus distintas manifestaciones. Si bien, sus principios generales resultan directamente aplicables, se constató la necesidad de contar con mayores precisiones (Fernández Delpech – Poullet – Pérez Asinari – Palazzi, 2009).

En tanto, el Poder Judicial frente a los mencionados desafíos tiene que dar respuestas a través de interpretaciones extensivas a nivel constitucional, a fin de poder proteger derechos vulnerados y no incluidos en leyes especiales. Siempre a través de la creación pretoriana de la Corte se han protegido derechos aún no tutelados.

Por lo expuesto, se van a analizar algunos fallos que tienen que ver con el hábeas data y de este modo se observa como la justicia considera y evoluciona en las nuevas cuestiones que se van planteando en lo relativo a las nuevas tecnologías.

3.1 Jurisprudencia nacional sobre habeas data. Casos relevantes.

a) Fallo Urteaga, Facundo Raúl c. Estado Nacional - Estado Mayor Conjunto de las FF.AA. – s/amparo ley 16.986[21]

El actor, Facundo R. Urteaga, interpuso recurso de Habeas Data para obtener los informes correspondientes a su hermano, quien había desaparecido en julio de 1976 en un supuesto enfrentamiento con las Fuerzas de Seguridad en la localidad de Villa Martelli, provincia de Buenos Aires. La información solicitada debía provenir de varios sectores correspondientes a registros estatales, militares, policiales o civiles a fin de que dieran cuenta de cómo se habían sucedidos los hechos, cuál fue el destino y donde se encontraban los restos de su hermano. En el caso de confirmarse que había sido asesinado, pedía determinar quiénes fueron los responsables del asesinato y en qué grado debía responder el Estado.

El juez de primera instancia rechazó la demanda interpuesta por considerar que la herramienta procesal del art. 43 de la Constitución Nacional solo puede ser utilizada por la persona a quien se refieren esos datos. Además, que por ese procedimiento en particular solamente se puede suprimir, rectificar, actualizar o asegurar la confidencialidad de los datos personales, lo que difiere con el objeto de la petición. El juez afirma que la vía procesal correcta es el Habeas Corpus, para el fin solicitado por el actor.

La sentencia de primera instancia fue apelada, la Cámara de Apelaciones (sala II) confirmó la sentencia, y argumenta la falta de legitimación (activa y procesal) y la diferencia de objeto en el instituto constitucional utilizado.

Ante esta nueva sentencia denegatoria el actor presentó recurso extraordinario. La Corte Suprema de Justicia de la Nación hace lugar al pedido del accionante y revoca la sentencia anterior, pero bajo dos recursos diferentes: recurso de amparo genérico y recurso de Habeas Data.

[21] C.S.J.N, "Urteaga, Facundo Raúl c/ Estado Nacional – Estado Mayor conjunto de las FF.AA. s/ amparo ley 16.986" Fallos 321:2767 (1998).

Los votos de los jueces de la Corte Suprema de Justicia traslucen algunos matices importantes desde el punto de vista jurídico.

Ya que para cinco jueces -EduardoMoliné O´Connor, Julio Nazareno, Adolfo Vázquez, Antonio Boggiano y Enrique Petracchi-, la vía procesal correcta para hacerlo es la acción de hábeas data, que fue la interpuesta por Facundo Urteaga. Al mismo tiempo sostienen que debe hacerse una interpretación amplia del hábeas data , para que no se frustre el derecho de buscar esa información, sobre la base de lo dispuesto en el artículo 43 de la Constitución Nacional, incorporado en la reforma de 1994. Así, sostuvieron que el objeto del recurso de F. Urteaga era el conocimiento de datos personales, por lo que corresponde la interposición del recurso de Habeas Data; ya que el accionante en primer lugar desea tomar conocimiento de los datos referidos al paradero de su hermano.

En cambio, los otros cuatro miembros del alto tribunal, Gustavo Bossert, Augusto Belluscio, Guillermo López y Carlos Fayt- sostuvieron que la vía correcta es la de la acción de amparo. Ya que sostuvieron que el actor no tenía legitimación para interponer el recurso de Habeas Data, el cual solo podía ser interpuesto por el titular de los datos, pero se admite que el actor es damnificado en cuanto a su derecho de conocer el paradero de su hermano o localizar sus restos.

Se debe tomar en cuenta que en el año 1998 no existía aún regulación legal sobre el procedimiento de Habeas Data que dispusiera quienes tenían legitimación activa a efectos de su interposición, ya que la Ley de Habeas Data es posterior, se sancionó en el año 2000.

Con este fallo la Corte Suprema de Justicia, admitió el derecho de los familiares de desaparecidos a buscar los datos que existan sobre las circunstancias que rodearon la muerte de aquellas personas y el destino de sus cadáveres. La importancia de este fallo radica, en que amplía la legitimación activa, otorgándoles acción a los hermanos, además del propio titular de los datos.

b) Fallo R. P., R. D. c/ Estado Nacional – Secretaría de Inteligencia del Estado – 19/04/2011 [22]

El actor entabló demanda de hábeas data con sustento en el artículo 43 de la Constitución Nacional, con el objeto de acceder a la información que, sobre su persona, obrase en el Servicio de Inteligencia del Estado (SIDE) con el objetivo de conocer si el mencionado organismo tenía en sus archivos información de interés para el cálculo de su jubilación del período comprendido entre 1961 y 1973, de acuerdo a lo que determina el decreto 4.827/58.

En esta causa se resolvió que al demandante le asiste el derecho a saber si la Secretaría de Inteligencia de la Presidencia de la Nación tiene en sus archivos información referente a sus datos personales, como así también que la jueza de primera instancia interviniente debía intimar a ese organismo para que remitiese la información requerida.

La Cámara advirtió que la jueza, a pedido del demandante, podía tomar conocimiento personal y directo de los actos que la SIDE reconociera tener, aunque con la obligación de mantener su confidencialidad, según lo previsto en el artículo 40, inciso 2º, de la Ley 25.326 (Ley de Protección de Datos Personales).

La Corte sostuvo, en sintonía con lo dictaminado por la Procuración General de la Nación, que la Constitución Nacional en su artículo 43 protege la identidad personal y garantiza que el interesado tome conocimiento de los datos referidos a él consignados y su finalidad, en registros públicos o privados que proveen informes. Además, lo autoriza, a exigir su supresión, rectificación, confidencialidad o actualización.

El alto tribunal rechazó el argumento del Estado, según el cual toda la información de inteligencia de la SIDE se halla contemplada en el artículo 17 de la ley 25.326, que permite denegar el suministro de datos cuando pudiera afectarse la defensa de la Nación, el orden o la seguridad pública.

[22] C.S.J.N., r. p., r. D. c/ Estado Nacional – Secretaría de Inteligencia del Estado, Fallos: 334:445 (2011)

Al respecto, expreso que excluir de la protección constitucional a esos datos comportaría la absurda consecuencia de ofrecer una acción judicial sólo en los casos en los que no es necesaria.

Asimismo, con este fallo la Corte Suprema de Justicia de la Nación estableció que el Sistema de Inteligencia Nacional debía ajustarse estrictamente a la Constitución Nacional, en sus capítulos I y II, y a las normas legales vigentes.

El fallo determinó que la Ley de Inteligencia Nacional (Ley 25.520) ordena a esa institución y a otras similares a enmarcar sus actividades dentro de las prescripciones generales de la Ley de Protección de los Datos Personales (Ley 25.326) y específicamente en lo que establece el artículo 23 de la mencionada norma legal.

Por lo tanto, la sentencia de la Corte Suprema de Justicia de la Nación fortalece la legislación vigente mediante una interpretación restrictiva de los casos en los que puede denegarse el acceso a la información de datos personales, almacenados en bases o registros de datos públicos pertenecientes a organismos del Estado.

c) Fallo Halabi, Ernesto c/ P.E.N. – ley 25.783 – dto. 1563/04 s/ amparo ley 16.986[23]

El actor o demandante interpuso una acción de amparo por considerar que las disposiciones de la ley 25.873 y de su decreto reglamentario 1563/04 vulneraban los derechos establecidos en los artículos 18 y 19 de la Carta Constitucional en la medida en que autorizan la intervención de las comunicaciones telefónicas y por Internet sin justificar en qué casos y con qué justificativos se podrían intervenir. La referida intervención importa una violación de sus derechos a la privacidad y a la intimidad, en su condición de usuario. Además, pone en serio riesgo el "secreto profesional" que como abogado se ve obligado a guardar y garantizar.

Es bueno recordar que la denominada Ley Nº 25873 -llamada Ley Espía- modificaba a la Ley 19.798 de Telecomunicaciones, bajo el pretexto de ser un instrumento necesario

[23] C.S.J.N., "Halabi Ernesto c/ P.E.N. ley 25.873 Dto. 1563/04", Fallos: 331:2784, (2008)

para investigar la comisión de ciertos delitos como el lavado de dinero, el tránsito y comercialización de estupefacientes y los secuestros de personas.

La norma, a requerimiento del Poder Judicial o el Ministerio Público, colocaba a su disposición el conocimiento de los contenidos de las comunicaciones telefónicas, o Internet, efectuadas por los usuarios, aunque no llegaran a estar involucrados en aquellos hechos delictivos.

Establecía que "los registros de tráfico de las comunicaciones cursadas" deberían conservarse por los prestadores de telecomunicaciones por el plazo de diez años. Esta norma generaba gran inseguridad jurídica dado que resulta incomprensible obligar a empresas privadas a que conserven información relativa a la privacidad de millones de personas, por un período de tiempo demasiado prolongado.

Una cosa es registrar a los emisores y destinatarios de las comunicaciones, que de por sí configura una lesión al derecho a la vida privada, y otra mucho más grave es permitir el funcionamiento de un sistema mediante el cual se pueden registrar los contenidos de tales comunicaciones y conservarlas durante diez años.

Tanto en primera como en segunda instancia se declaró la inconstitucionalidad de la norma mencionada y cuestionada. Fue la Cámara de Apelaciones, que al confirmar el fallo, consideró que la cuestión no se había vuelto abstracta, aunque el decreto cuestionado había sido suspendido por otro decreto en el 2005, pero no derogado. Además, el tribunal de apelaciones señaló que el Estado esgrimió argumentos demasiados débiles para mantener así la validez de una norma demasiado controvertida.

Entonces, frente a este fallo adverso, el Estado nacional dedujo recurso extraordinario y así fue que el caso llegó a la Corte Suprema.

La Corte Suprema de Justicia declaró la inconstitucionalidad de la ley 25.873 que autorizaba la intervención de las comunicaciones telefónicas y por Internet, con la obligación de las empresas de preservar durante 10 años la información sobre las comunicaciones de los usuarios.

El fallo, dictado por la mayoría de los miembros del tribunal, confirmó sentencias de primera y segunda instancia del fuero en lo Contencioso Administrativo que ya habían declarado inconstitucional la ley 25.873 y su decreto reglamentario. Los magistrados entendieron que las comunicaciones a las que se refiere la mencionada ley integran la esfera de la intimidad de las personas y se encuentran protegidas por los artículos 18 y 19 de la Constitución Nacional.

Sobre este fallo se han referido distintos doctrinarios:

"Nos parece muy positivo que la Corte ampare la privacidad y que lo haga de manera tan tajante, incluso cuando procesalmente no tenía que hacerlo (la cuestión había quedado firme en la instancia anterior). Es importante semejante postura de la Corte Suprema por lo invasiva que resultan hoy en día las tecnologías de la información y porque seguramente a futuro nos encontraremos con planteos similares. A mayores peligros, la respuesta de los tribunales debe ser siempre reforzar las garantías constitucionales" (Fernández Delpech – Poullet – Pérez Asinari – Palazzi, 2009, p.49).

> En sus considerandos, el fallo de marras expone su preocupación por lo que denomina "tensión" entre las nuevas Tecnologías de la información y las Comunicaciones (TIC) y el derecho a la intimidad. Así dice: "Todo lo concerniente al desarrollo de las nuevas tecnologías de las comunicaciones, (especialmente: Internet, correo electrónico, etc.) y las tensiones que ello dispara de cara a la protección del derecho a la intimidad de datos personales, de la seguridad (incluida la salvaguarda de la defensa nacional, los intereses del consumidor y la defensa de la competencia), es motivo de creciente preocupación y debate en el derecho comparado y en numerosos juristas especializados en las más variadas disciplinas" (Rodolfo D. Uicich, 2009, pág. 149).

Con este fallo la Corte Suprema de Justicia de la Nación creó " la acción de clase" para proteger derechos homogéneos, en la que se analizó la inconstitucionalidad de las normas que autorizaban la intervención de comunicaciones telefónicas y por Internet.

La decisión del Máximo Tribunal permite así que una sentencia tenga efectos para todos los ciudadanos -efecto erga omnes- que padecen un mismo problema, sin la necesidad de tener que iniciar un juicio.
Esta sentencia tiene dos aspectos de gran relevancia: a) por un lado crea la acción de clase, esto es una garantía de los derechos de dimensión colectiva, y b) por otro protege la privacidad en el uso de Internet y telefonía personal frente a posibles intromisiones de organismos del Estado.

d) Fallo María Belén Rodríguez contra *Google Inc. s/* daños y perjuicios[24]

La actora o demandante María Belén Rodríguez promovió demanda de daños y perjuicios contra *Google Inc.* (Google) –después ampliada contra *Yahoo* de *Argentina SRL* (Yahoo)– en la que sostuvo que se había procedido al uso comercial y no autorizado de su imagen y que también, se habían avasallado sus derechos personalísimos al habérsela vinculado a determinadas páginas de Internet de contenido erótico y/o pornográfico. Pidió el cese de tal uso y la supresión de las vinculaciones a tales páginas de Internet.

Los derechos en conflicto por un lado, la libertad de expresión e información y, por el otro, el derecho al honor y a la imagen.

La sentencia dictada en primera instancia por el Juzgado Nacional de Primera Instancia en lo Civil N° 95, hizo lugar a la demanda y consideró que las demandadas habían incurrido en negligencia culpable "al no proceder a bloquear o impedir de modo absoluto la existencia de contenidos condenó a Google a pagar $ 100.000 y a Yahoo $ 20.000, y además dispuso que se efectuase "la eliminación definitiva de las vinculaciones del nombre, imagen y fotografías de la actora con sitios y actividades de contenido sexual; erótico y/o pornográfico".

El fallo fue apelado, a su turno la Sala A de la Cámara Nacional de Apelaciones en lo Civil lo revocó parcialmente, ya que rechazó el reclamo contra *Yahoo* y lo admitió contra Google reduciendo –en este último caso– la indemnización a la suma total de $

[24] C.S.J.N., María Belén Rodríguez contra *Google Inc. s/* daños y perjuicios (2014)

50.000, al tiempo que dejó sin efecto el pronunciamiento de primera instancia en cuanto éste disponía la eliminación de las mencionadas transcripciones. Esta decisión se basó en la consideración de que correspondía encuadrar la eventual responsabilidad de los llamados "motores de búsqueda" (como Google y *Yahoo)* en el ámbito de la responsabilidad subjetiva y descartó que pudiera aplicarse el art. 1113 del Código Civil en la parte que alude al "riesgo".

Sí condenó a Google, en el tema relativo a los llamados *thumbnails* que contenían la imagen de la actora, por entender que Google debía haber requerido el consentimiento de aquélla, de acuerdo a lo impuesto por el art. 31 de la ley 11.723.

Asimismo, estimó que el eventual damnificado debe notificar puntualmente al "buscador" sobre la existencia de contenidos nocivos en una página web determinada y ello "no admite, por consiguiente, una orden genérica de la extensión de la contenida en la sentencian, por lo que esta última fue revocada en ese punto.

Debido a tal pronunciamiento la parte actora y Google interpusieron sendos recursos extraordinarios, que fueron concedidos por la cámara solo en cuanto estaba en juego la inteligencia de derechos de raigambre constitucional y los denegó por la causal de arbitrariedad invocada.

Luego, en el fallo, la Corte Suprema de Justicia de la Nación, por mayoría, resolvió desestimar el recurso extraordinario de la actora y hacer lugar al deducido por el buscador Google demandado, revocando parcialmente la sentencia apelada, dictada por la Sala A de la Cámara Nacional de Apelaciones en lo Civil.

Este fallo es interesante y sienta precedentes ya que luego de un extenso debate tanto jurisprudencial como doctrinario, acerca del tipo de responsabilidad civil que corresponde a los buscadores de internet, y ante la inexistencia de previsión legal sobre el tema, la Corte Suprema de Justicia de la Nación ha determinado su posición al respecto, en el fallo "María Belén Rodríguez contra Google Inc. s/ daños y perjuicios".

En lo que se relaciona a los motores de búsqueda, la Corte Suprema de Justicia de la Nación establece que éstos tienen un rol de gran importancia en el funcionamiento de Internet. Así, para sostener dicho argumento cita un fallo del Tribunal de Justicia[25] de la Unión Europea, en el cual se señaló que "la actividad de los motores de búsqueda desempeña un papel decisivo en la difusión global de dichos datos en la medida en que facilita su acceso a todo internauta que lleva a cabo una búsqueda a partir del nombre del interesado, incluidos los internautas que, de no ser así, no habrían encontrado la página web en la que se publican estos mismos datos".

En lo referente a responsabilidad objetiva versus responsabilidad subjetiva:

la CSJN continúa su análisis, y procede a definir si el caso concreto debe ser analizado bajo las reglas de la responsabilidad objetiva, como lo pretende la actora, o bajo la órbita de la responsabilidad subjetiva tal como fuera fallado por el tribunal de grado.

Para lo cual también, realiza un análisis del derecho comparado en lo que se refiere a la definición de los motores de búsqueda y sobre legislación específica que tienen ciertos países del mundo en relación a estos temas. Adopta así, la definición de motores de búsqueda dominante en el derecho comparado, la cual establece que "Los «motores de búsqueda» (search engines) son los servicios que buscan automáticamente en Internet los contenidos que han sido caracterizados por unas pocas «palabras de búsqueda» (search words) determinadas por el usuario. Su manera de funcionar los caracteriza como una herramienta técnica que favorece el acceso al contenido deseado por medio de referencias automáticas".

Luego, prosigue con un análisis de la legislación existente en ciertos países del mundo que específicamente regulan la responsabilidad de los motores de búsqueda.

Finalmente, concluyen que en general se afirma que los buscadores no tienen una obligación general de monitorear los contenidos que se suben a la red ya que los mismos son provistos por los responsables de cada una de las páginas web, y, sobre esta base, se fundamenta que, los motores de búsqueda no son responsables por los contenidos que no han creado.

[25] Google Spain S.L. Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González", 13/05/2014

Para concluir con sus fundamentos en cuanto a la improcedencia de analizar el caso bajo los términos de la responsabilidad objetiva, la CSJN cita un fallo de la Royal Courts of Justice[26], el cual, de forma muy clara, expresa que: "responsabilizar a los «buscadores» como principio por contenidos que no han creado, equivaldría a sancionar a la biblioteca que, a través de sus ficheros y catálogos, ha permitido la localización de un libro de contenido dañino, so pretexto que habría «facilitado» el daño. Más allá de que la sanción sería injusta, es muy probable que de seguirse ese criterio «objetivo» de responsabilidad, terminarán cerrándose muchas bibliotecas, con gran perjuicio de los lectores".

Entonces, la Corte Suprema de Justicia de la Nación establece que la pretensión de aplicar los principios de la responsabilidad objetiva al caso "María Belén Rodríguez contra Google Inc. s/ daños y perjuicios", es de una llamativa insustancialidad, y afirma que la libertad de expresión sería mellada de admitirse la responsabilidad objetiva que, por definición, prescinde de toda idea de culpa, y en consecuencia, de juicio de reproche a aquél a quien se endilga la responsabilidad.

Para concluir, la Corte Suprema de Justicia de la Nación determina con esta sentencia, que corresponde juzgar la eventual responsabilidad de los "motores de búsqueda" bajo lo establecido para la responsabilidad subjetiva. Ya que – de conformidad con la tendencia dominante en el derecho comparado- los buscadores no tienen una obligación general de monitorear los contenidos que se suben a la red y que son proveídos por los responsables de cada una de las páginas web. En consecuencia, toda vez que actúan como meros intermediarios se concluye en que son, no responsables por aquellos contenidos que no ha sido creado por ellos.

Pero, la CSJN destaca que en algunos casos los buscadores podrían llegar a responder por un contenido que le es ajeno, y sería a partir del momento en que se produce el efectivo conocimiento del contenido ilícito de una página web, al no procurar los buscadores el bloqueo del resultado, serían responsables por culpa.

En lo que se relaciona a la determinación del factor de atribución subjetivo para atribuir responsabilidad a un buscador, la CSJN se ha expedido acerca del "efectivo conocimiento requerido para la responsabilidad subjetiva", manifestando que en

[26] Metropolitan International Schools Ltd. v. Google Inc., Court of Appeal-Queen' s Bench Division, Royal Courts of Justice, Strand, London, WC2A 2LL16-07-2009.

aquellos casos donde el daño resulte manifiesto y grosero bastaría la simple notificación privada –pero siempre de manera fehaciente-; y en aquellos casos donde el contenido dañoso exija un esclarecimiento, para que el buscador tenga conocimiento acerca de la supuesta ilicitud, es necesaria la notificación del hecho en sede judicial o administrativa.

Se considera valedero mencionar que es, en este juicio que el Dr. Granero, abogado especializado en Derecho de la Alta Tecnología, se presentó como AMICUS CURIAE (art. 9º del Reglamento sobre Intervención de Amigos del Tribunal Ac. CSJN 7/2013), en la que manifiesta su apoyo a la teoría de la responsabilidad objetiva, ya que considera a la actividad de los buscadores peligrosa para terceros y explica que el riesgo de la actividad, debe realizarse en abstracto, con total prescindencia del juicio de reprochabilidad subjetiva que podría merecer la conducta del sindicado como responsable en el caso concreto.

La Corte Suprema de Justicia de la Nación consideró que no correspondía juzgar responsabilidad de los motores de búsqueda de acuerdo a las normas que establecen la responsabilidad objetiva, sino que se lo debe hacer bajo los parámetros establecidos en la responsabilidad subjetiva.

Personalmente considero que en un futuro cercano habrá fallos en que se considere válido aplicar el artículo 1757 del Código Civil y Comercial que establece: "toda persona responde por el daño causado por el riesgo o vicio de las cosas, o de las actividades que sean riesgosas o peligrosas por su naturaleza, por los medios empleados o por las circunstancias de su realización. La responsabilidad es objetiva. No son eximentes la autorización administrativa para el uso de la cosa o la realización de la actividad, ni el cumplimiento de las técnicas de prevención."

Reflexiono que las nuevas formas de riesgos no pueden contenerse en el esquema tradicional de la responsabilidad por culpa, simplemente porque en la era tecnológica los siniestros conciernen o van a concernir a la actividad riesgosa o al riesgo de la cosa.

3.2 Jurisprudencia extranjera

a) Fallo Google Spain, S.L., Google Inc. y Agencia Española de Protección de Datos (AEPD) Mario Costeja González[27]

El Tribunal de Justicia de la Unión Europea (TJUE) ha fallado que el principal buscador del mundo está obligado a retirar resultados de búsqueda a petición de un ciudadano si los sitios web a los que se enlaza contienen datos personales del solicitante, incluso si el sitio web de origen no elimina dicha información o ésta es lícita.

Esto supone un importante respaldo al llamado "derecho al olvido", es decir, la posibilidad de un ciudadano de borrar sus datos personales y su "rastro" en la Red.

La decisión del Tribunal de Luxemburgo contesta en su sentencia a nueve preguntas planteadas por la Audiencia Nacional, a raíz de un recurso de Google contra una decisión de la Agencia Española de Protección de Datos (AEPD). Esas preguntas se pueden resumir en tres bloques:

1-¿Puede el usuario dirigirse directamente a Google en el caso de modificación o cancelación de los datos que el buscador "indexa"? La respuesta es sí, dado que Google es considerado en parte responsable de dichos datos.

2-¿Lo que realiza Google puede considerarse como 'tratamiento de datos'? La respuesta es sí, dado que "recoge" tales datos que "extrae", "registra" y "organiza" posteriormente en el marco de sus programas de indexación, "conserva" en sus servidores y, en su caso, "comunica" y "facilita el acceso" a sus usuarios en forma de listas de resultados. "La propia presentación de datos personales en una página de resultados de una búsqueda constituye un tratamiento de tales datos", dice la sentencia.

3-¿Se ha de aplicar en este caso la normativa europea sobre protección de datos? La respuesta es que sí, dado que Google trata datos personales y las filiales de Google en Europa son consideradas "establecimientos" en el sentido de la Directiva 95/46, y aunque la actividad de búsqueda no realiza tratamiento de datos personales en España el Tribunal considera sí se realizan "en el marco de las actividades" de dicho "establecimiento".

La sentencia establece que el derecho a la protección de datos de las personas prevalece, con carácter general, sobre el "mero interés económico del gestor del motor de

[27] http://www.elmundo.es/tecnologia/2014/05/13/5371d458268e3e67508b456e.html

búsqueda" salvo que el interesado tenga relevancia pública y el acceso a la información esté justificado por el interés público.

b) Recientemente un tribunal de apelaciones en Estados Unidos determinó que las autoridades nacionales no pueden forzar a la empresa de informática Microsoft [28]a entregarles información contenida en servidores alojados en otros países.

Hechos:

El caso llegó a los tribunales después de que Microsoft se negara a otorgarle acceso al Departamento de Justicia de Estados Unidos, a un servidor ubicado en Irlanda. El pedido de acceso tenía que ver con una investigación relacionada con estupefacientes. Un tribunal de Manhattan en primera instancia, le dio la razón al Departamento de Justicia en 2014. Pero la Corte de Apelaciones deshizo esa decisión.

El Departamento de Justicia rechazó el fallo e indicó que estaba evaluando la posible apelación. En caso afirmativo el caso lo tendrá que resolver la Corte Suprema de Justicia.

La importancia del fallo radica en que sienta un precedente histórico en materia de protección de la privacidad para servicios de computación en la nube.

Además, deja claro que el gobierno de Estados Unidos no puede utilizar órdenes judiciales en forma unilateral para llegar a otros países y obtener los correos electrónicos que pertenecen a personas de otras nacionalidades.

Se considera que el derecho a la privacidad individual, es de mayor importancia y está protegido frente a la intrusión del Estado.

En consecuencia, los organismos de seguridad de Estados Unidos deben respetar el derecho a la privacidad digital de los ciudadanos europeos y la protección de sus datos personales.

[28] http://www.lanacion.com.ar/1918873-microsoft-gano-una-sentencia-historica-para-no-tener-que-entregar-datos-privados-de-sus-usuarios-a-las-autoridades

El magistrado, Gerard Linch, afirmó "que la Ley de 1986 necesita una actualización urgentemente".

En suma, se puede afirmar que a nivel mundial, la protección de la privacidad y las necesidades de las autoridades a cargo de hacer cumplir la ley requieren de nuevas soluciones que reflejen al mundo actual, en vez de tecnologías que existían hace tres décadas, cuando se aprobaron las leyes que están vigentes.

Conclusión

Podemos concluir que el habeas data antes de ser receptado en la reforma del año 1994 ha surgido de la creación pretoriana de la Corte Suprema de Justicia a través de un fallo trascendental como es el Fallo Ponzetti de Balbín, donde se resguarda el derecho a la intimidad por sobre el abuso en el ejercicio del derecho o libertad prensa.

Más tarde en 1998, la Corte analiza el caso Urteaga en donde se amplía la legitimación a los hermanos en su "derecho a conocer" sobre el paradero de sus familiares, además del propio titular de los datos.

Con el fallo R. P., R. D. c/ Estado Nacional –Secretaría de Inteligencia del Estado– estableció que el Sistema de Inteligencia Nacional debía ajustarse estrictamente a la Constitución Nacional, en sus capítulos I y II, y a las normas legales vigentes.

El mencionado fallo evocó que la Ley de Inteligencia Nacional (25.520) ordena a esa institución y a otras similares a enmarcar ineludiblemente sus actividades dentro de las prescripciones generales de la Ley de Protección de los Datos Personales (Ley 25.326) y específicamente en lo que establece el artículo 23 de la mencionada norma legal.

Con el fallo Halabi, la Corte Suprema de Justicia de la Nación creó la acción de clase para proteger derechos homogéneos, en la que se analizó la inconstitucionalidad de las normas que autorizaban la intervención de comunicaciones telefónicas y por Internet.

La decisión del Máximo Tribunal permite así que una sentencia tenga efectos para todos los ciudadanos -efecto erga omnes- que padecen un mismo problema, sin la necesidad de tener que iniciar un juicio. Entonces, se amplía la legitimación, aceptándose la legitimación colectiva y el efecto erga omnes de la sentencia, algo novedoso porque hasta ese momento solo afectaba o beneficiaba a la persona que interponía la demanda.
En el fallo María Belén Rodríguez contra *Google Inc. s/* daños y perjuicios, la Corte Suprema de Justicia de la Nación señaló que este caso ponía en conflicto dos grupos de derechos: "por un lado, la libertad de expresión e información, y, por el otro, el derecho al honor y a la imagen".

Al dictar esta sentencia la CSJN consideró que no correspondía juzgar la responsabilidad de los motores de búsqueda de acuerdo a las normas que establecen la responsabilidad objetiva, sino que se lo debe hacer bajo los parámetros establecidos en la responsabilidad subjetiva.

El fallo no fue unánime, y tuvo voto en disidencia parcial de Ricardo Lorenzetti y Juan Carlos Maqueda, que consideraron que los buscadores deben eliminar o bloquear "enlaces que resulten claramente lesivos de derechos personalísimos" y adoptar "las medidas necesarias" para "evitar que en el futuro se establezcan nuevos vínculos de igual tipo". Y el voto de la mayoría, estuvo integrado por Elena Highton de Nolasco, Eugenio Raúl Zaffaroni y Carlos Fayt.

Así, se observa en este fallo que las nuevas tecnologías nos interpelan básicamente en el conflicto constitucional que se presenta entre el derecho al honor, la imagen y la intimidad, por un lado y por el otro, el derecho a la libertad de expresión.

Esto nos lleva a afirmar que muchas veces nos encontramos frente a una mora del legislador en temas de importancia y que son tratados con mayor celeridad por la justicia frente a planteamientos de los particulares en defensa de derechos constitucionales tutelados. Tenemos al final del capítulo jurisprudencia muy actual, especialmente en el caso de la empresa Microsoft donde se encuentra involucrado uno de los países más poderosos del mundo, y que frente a los avances tecnológicos su legislación es anticuada y piden su pronta modificación.

Es casi nulo en materia jurisprudencial el tema de la protección de los datos personales en lo que se llama computación en la nube. Por lo pronto es preciso comenzar a trabajar en la modificación o creación de leyes sobre protección de datos y visualizar los nuevos retos que se presentan en la realidad, con el objeto de brindar las herramientas necesarias al poder judicial.

Capítulo 4 La Ley 25326. Su aplicación al tratamiento de datos personales por parte de terceros en entornos *cloud computing*

Introducción

Aristóteles define el arte o tecnología como "el hábito productivo acompañado de razón verdadera" (Granero, 2003, p.11).

Mientras que Santo Tomás la define como "el arte no es otra cosa que la recta razón de algunos objetos que deben hacerse. Ahora bien, el bien de estas cosas depende, no de la disposición del apetito humano, sino de la misma bondad de la obra realizada" (Granero, 2003, p.12).

Entonces, el hombre busca realizar instrumentos –en este caso tecnología– para su bienestar, para alivianar su trabajo, goce, entre otros, los cuales constituyen medios para facilitar la vida del hombre. Estas cosas que son el objetivo o fin de la tecnología, son, para la prudencia, medios. Ya que la búsqueda del bien total del hombre, aquel que se refiere a todas sus dimensiones humanas, no es objeto del arte sino de la prudencia.

La prudencia procura la felicidad, sin embargo, con felicidad no se hace referencia a un concepto determinado sino al logro del proyecto de vida que tiene cada persona, más allá de un sentimiento de placer. En realidad se apunta a la realización personal, al fin último de las personas. Este es un concepto filosófico y de origen aristotélico, que apunta a entender que cada uno busca ser pleno.

Es así que al analizarse la ley de habeas data (Ley Nº 25326), se tendrá en cuenta que debe haber en el obrar humano, y por supuesto en la tecnología, sujeción al orden ético.

"La ética es un tipo de saber de los que pretende orientar la acción humana en un sentido racional" (Cortina, 2000, p. 17)

La ética actúa sobre la conducta humana y en el momento en que se toma una decisión pone en juego valores (por ejemplo: la honestidad, el respeto, la justicia), pensamientos y afecta a otras personas siempre. Por eso se dice que es un saber práctico: actúa directamente sobre la conducta humana. Generalmente está presente en todos los momentos de la vida: en las situaciones personales y también en los ámbitos laborales.

Se debe tener en cuenta que el resultado de este proceso de reflexión debe ser una decisión, que para ser ética, debe ser prudente y justa.

Por prudente se refiere a que la ética busca el estilo de vida procurando la felicidad de las personas. Como expresa Adela Cortina, "la ética hace que la vida valga la pena ser vivida" (Cortina, 2000, p. 19).

Esa decisión a tomar también debe ser justa; con justicia se hace referencia a la manera en que las decisiones afectan a los demás. Cada vez que se decide algo se está afectando de alguna manera a otra persona o a un grupo de personas.

Entonces, se puede decir que la tecnología se encuentra subordinada a la ética, ya que la tecnología sabe cómo hacer las cosas, pero solo el saber ético puede decir qué cosas han de hacerse y cuáles no han de hacerse.

Al referirse a tecnología, es indudable que la informática y las comunicaciones electrónicas evolucionan, desplazan y revolucionan de modo incesante, llevándose por delante décadas de tradiciones, costumbres y leyes, ya que pone en tela de juicio al derecho al dejar desactualizada longevas normas jurídicas y otras no tan longevas sino más bien recientes. Pero, justamente es una de las características más sobresalientes de la tecnología, su gran avance a una velocidad vertiginosa e inimaginable.

Por lo cual se abordará en un breve análisis los artículos más relevantes y que inciden de manera más preponderante en el tratamiento de los datos personales cuando los mismos son tratados en las llamadas "*cloud computing*" o computación en la nube, para más tarde determinar si es necesaria la modificación de la Ley Nº 25326 o no. Como ya se mencionó, el *cloud computing* o computación en la nube, es un modo de prestación de servicios informáticos, el cual es el resultado de la evolución de muchas tecnologías, que permite ofrecer la informática como un servicio disponible a través de Internet.

La ley de habeas data o de protección de datos personales (Ley Nº 25326 o LPDP) asume que el tratamiento de los datos personales implica de por sí ciertos riesgos para los derechos personales de los registrados. En este punto, se consideraran especialmente los siguientes artículos:

a) Artículo 9 - Seguridad de los datos.

b) Artículo 10 - Deber de confidencialidad.

c) Artículo 11- Cesión.

d) Artículo 12 -Transferencia internacional.

e) Artículo 25 -Prestación de servicios informatizados de datos personales.

Entonces, de este modo se analizará la protección de los datos personales cuando los mismos son tratados en entornos de servicios *cloud computing* y más aún se pondrá el énfasis cuando los mismos son tratados por terceros. El análisis se delimita a las relaciones B2B -*Business to Business,* en inglés- producto de la externalización de servicios de TI, en las que, en consecuencia, el cliente es el responsable del tratamiento y el proveedor de *cloud computing* es un mero encargado de tratamiento que actúa bajo las instrucciones del primero.

4.1- Análisis de la transferencia internacional de datos personales

Generalmente, contratar servicios en entornos *cloud computing* implica la transferencia internacional de datos personales. Por lo que el control de los datos personales deja de estar bajo el dominio del usuario –responsable– y entra en la órbita de un tercero. Debido a que las actividades que se relacionan con la prestación de servicios *cloud computing* poseen en su gran mayoría una dimensión internacional porque la tecnología que se utiliza en ello es generalmente importada debido a que los proveedores son extranjeros, principalmente de Estados Unidos.

Ya en diciembre de 2001 expresaba Palazzi: “la información es un bien muy difícil de regular, más aún cuando a través de Internet puede quedar sujeta a varios ordenamientos jurídicos conflictivos entre sí. Es por ello que en el estado actual de la cuestión un análisis del derecho a la privacidad no puede prescindir de una visión global y de las tensiones que dentro de cada continente han llevado a regular la privacidad y los flujos de datos internacionales” (Palazzi, 2001, p. 20).

Se puede decir que una transferencia internacional de datos personales, es necesariamente un tipo de procesamiento de datos que consiste en la transmisión de datos, fuera de los límites geográficos de un Estado, realizado por una organización (empresaria, bancaria u otra) -que es la responsable del tratamiento– a una persona jurídica o física, que los recibirá en un tercer país, entonces los datos pasan a estar alcanzados por otra normativa jurídica. Los motivos de la transferencia pueden ser una cesión, una prestación de servicios o una transmisión internacional entre distintas sedes de una misma organización empresarial.

Se observa, entonces, la intervención de dos sujetos:

1) un exportador de los datos (transmisor argentino o responsable), es justamente el responsable de la transferencia de los datos personales fuera del país.

2) y un importador de los mismos, es quien recibe los datos del exportador para su almacenamiento o su tratamiento, de acuerdo a lo convenido con él.

La Ley Nº 25326 no contiene una definición expresa del concepto de transferencia. No obstante, se encuentra tanto en el artículo 11 (Cesión) como el artículo 12 (Transferencia internacional) de la mencionada ley, que hacen referencia a la situación que se produce cuando los datos salen de la base de datos original y pasan a un tercero.

La ley que rige las telecomunicaciones en nuestro país es la Ley Nº 19798 (Ley Nacional de Telecomunicaciones) y en el artículo 2 define el concepto de telecomunicación como: "Toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza, por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos". Y además especifica que "Todo vocablo o concepto no definido en esta ley, tiene el significado establecido en los convenios y reglamentos nacionales e internacionales". Se puede hablar de que la Ley 19798 es transversal es decir que atraviesa a la Ley 25326 por la amplitud del concepto de telecomunicación.

Según el diccionario de la RAE transmitir significa: "Trasladar, transferir". Otra acepción es: "Conducir o ser el medio a través del cual se pasan las vibraciones o radiaciones".

Y si se recuerda el concepto de tratamiento de datos, definido en el artículo 2 de la Ley Nº 25326 es: "Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, como así también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias".

Por lo tanto, se puede ya tener una mejor apreciación o aproximación al concepto de transferencia para así considerar los artículos mencionados como los más relevantes para la temática que se aborda en el presente trabajo[29].

Artículo 11 - Cesión

En el **artículo 11** se trata el tema de la cesión que es el traslado de toda la base de datos personales o parte de ella a otra base de datos. Este artículo señala de manera precisa que: "Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario…" y luego añade dos condiciones muy importantes que son las siguientes:

a) el previo consentimiento del titular de los datos – Y de acuerdo al artículo 5 de la ley 25326, el consentimiento debe ser libre expreso e informado y deberá constar por escrito o por otro medio que permita se le equipare, de acuerdo a las circunstancias– y

b) se le debe notificar al titular de los datos, sobre la finalidad de la cesión y debe poder identificar al cesionario o se le debe brindar los elementos que permitan hacerlo.

Cabe aclarar que el mencionado consentimiento es revocable.

En el inciso 3 del artículo 11, se fijan las excepciones respecto a los casos en que no es necesario el consentimiento del titular de los datos.

[29] Se tendrá en cuenta el libro de Pablo Palazzi, "La protección de los datos personales en la Argentina"

Otra precaución que establece la ley en el inciso 4 del artículo 11, es para garantizar el control de datos personales, ya que el cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias que el cedente y este último responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate. Entonces, queda establecida la solidaridad del cedente y del cesionario para los casos de violación a la presente ley. No obstante, el decreto reglamentario establece lo siguiente: "El cesionario a que se refiere el artículo 11, inciso 4, de la Ley Nº 25326, podrá ser eximido total o parcialmente de responsabilidad si demuestra que no se le puede imputar el hecho que ha producido el daño.". Sin embargo, se le puede aplicar el artículo 1757 del nuevo Código Civil y Comercial sobre riesgo creado, y la responsabilidad es objetiva.

Artículo 12- Transferencia internacional

En lo referente al **artículo 12** –transferencia internacional–, la diferencia sustancial se da cuando los datos salen de la base de datos original y pasan a un tercero, pero, para que se aplique este artículo será necesario que ese tercero esté fuera de la Argentina. Y para que sea lícita la transferencia debe tratarse de una jurisdicción que proporcione una legislación con niveles de protección adecuada o equiparable a la de nuestro país.

Se resalta que es responsabilidad del transmisor argentino –exportador de los datos– verificar las condiciones del país receptor en lo que se refiere legislación adecuada.

Nuestra ley incluyó pocas excepciones[30] en el mencionado artículo 12. Asimismo, el decreto reglamentario amplía dichas excepciones a dos supuestos[31] más. El mencionado

[30]La prohibición no rige en los siguientes supuestos: a) Colaboración judicial internacional; b) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica, en tanto se realice en los términos del inciso e) del artículo 11 de la Ley 25326; c) Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable; d) Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte; e) Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

[31] a) cuando el titular de los datos hubiese prestado su consentimiento expreso a la cesión y b) cuando se trate de la transferencia desde un Registro Público legalmente constituido abierto a la consulta del público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones legales y reglamentarias para la consulta.

Decreto1558/2001 faculta a la Dirección Nacional de Protección de Datos Personales a evaluar, de oficio o a pedido de parte interesada, el nivel de protección proporcionado por las normas de un Estado u organismo internacional. Además, el mismo decreto establece ciertas pautas que permiten decir si un país es adecuado o no a los fines de una transferencia, lo cual fue omitido en el artículo 12 de la ley. De la reglamentación se desprende que se evaluará todas aquellas circunstancias relevantes en una transferencia o en una categoría de transferencias de datos tomando en cuenta la naturaleza de los datos, su finalidad y la duración del tratamiento o de los tratamientos previstos, el lugar de destino final y las medidas de seguridad en vigor en dichos lugares, o que resulten aplicables a los organismos internacionales o supranacionales.

En este punto, también es pertinente mencionar la **Disposición 60 - E/2016** de la Dirección Nacional de Protección de Datos Personales (DNPDP), que basándose en el mencionado artículo 12 del Anexo I del Decreto N° 1558/01, establece en su artículo 2º lo siguiente: "Dispónese que aquellos responsables de tratamiento que efectúen transferencias de datos personales a países que no posean legislación adecuada en los términos del artículo 12 de la Ley N° 25326 y su Decreto reglamentario N° 1558/01, y utilicen contratos que difieran de los modelos aprobados en el artículo anterior o no contengan los principios, garantías y contenidos relativos a la protección de los datos personales previstos en los modelos aprobados, deberán solicitar su aprobación ante esta Dirección Nacional presentándolos, a más tardar, dentro de los Treinta (30) días corridos de su firma".

En el artículo 3° de la mencionada disposición se establece qué países presentan una legislación adecuada[32].

Expresó Palazzi[33] sobre la misma:

---

[32] "A los fines de la aplicación de la presente disposición se consideran países con legislación adecuada a los siguientes: Estados miembros de la Unión Europea y miembros del espacio económico europeo (EEE), Confederación Suiza, Guernsey, Jersey, Isla de Man, Islas Feroe, Canadá sólo respecto de su sector privado, Principado de Andorra, Nueva Zelanda, República Oriental del Uruguay y Estado de Israel sólo respecto de los datos que reciban un tratamiento automatizado. Esta enumeración será revisada periódicamente por esta Dirección Nacional, publicando la nómina y sus actualizaciones en su sitio oficial en Internet".

La nueva normativa aprobada por la DNPDP en el 2016 era muy esperada y nos parece que tendrá un resultado positivo en la práctica de esta nueva rama del Derecho. Facilita el intercambio de datos personales mediante la creación de dos modelos contractuales tipo que las empresas o personas podrán usar. Esto es de gran ayuda para pequeñas y medianas empresas. Asimismo determina en forma clara cuáles son los destinos adecuados en materia de protección de datos, algo que la DNPDP nunca había hecho antes. De esa forma se clarifica que a países adecuados como los miembros de la UE o aquellos reconocidos por ese bloque regional no se requiere un contrato para transferir datos en forma internacional, sin perjuicio de que las partes quieran documentar la transferencia.

Artículo 9 - Seguridad de los datos

En el **artículo 9** se legisla sobre la seguridad de los datos personales, debido a los riesgos que presenta tanto con la transferencia de los datos como con la misma seguridad de estos. Es por ello que este principio está presente en la mayoría de las leyes de protección de datos del Derecho comparado.

El responsable del archivo o banco de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad e integridad de los datos personales. Cuando se habla de seguridad, justamente se trata de garantizar mediante el uso de medidas técnicas y de la organización, a fin de evitar adulteración, pérdida, tratamiento no autorizado, y al mismo tiempo se debe poder detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

Cabe aclarar que no es fácil distinguir a las medidas de seguridad técnicas de las organizativas. Las medidas técnicas tratan sobre el uso práctico de métodos implementados para asegurar los datos tratados, incluyendo la prevención de acceso físico al hardware y software. Mientras que las medidas organizativas se refieren a un conjunto de reglas que permiten la seguridad de los datos al reglamentar los

[33] http://www.udesa.edu.ar/sites/default/files/la_ley_15.2.2017_2.pdf

procedimientos de autorización y autenticación. También en la formación e información adecuada al personal, empezando por los directivos para que como en cascada afecte a todos los niveles de la organización.

Además, quien trata datos personales de terceros debe adoptar las precauciones necesarias para evitar fugas o salidas de información y la consecuente revelación negligente de datos personales. Ya que si ello ocurriese, el responsable del tratamiento deberá responder por su impericia en el tratamiento o procesamiento de datos personales, es decir por los daños que ocasione su negligencia.

Aquí, cabe recordar que la seguridad informática concierne a la protección de la información que se encuentra en una computadora o en una red de ellas y también a la protección del acceso a todos los recursos del sistema.

De acuerdo al inciso 2 del artículo 9, queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.

De acuerdo al diccionario de la RAE "integro" significa: "Que no carece de ninguna de sus partes". Justamente, al hablar de integridad –en Informática o Tecnología– se hace referencia al estado de corrección y completitud de los datos ingresados en una base de datos. Para lo cual se suele utilizar la validación de datos, la cual hace referencia a verificar, controlar o filtrar cada una de las entradas de datos que provienen desde el exterior del sistema informático para luego, recién ser dadas de alta, baja o modificaciones en los registros de la mencionada base de datos, según el caso.

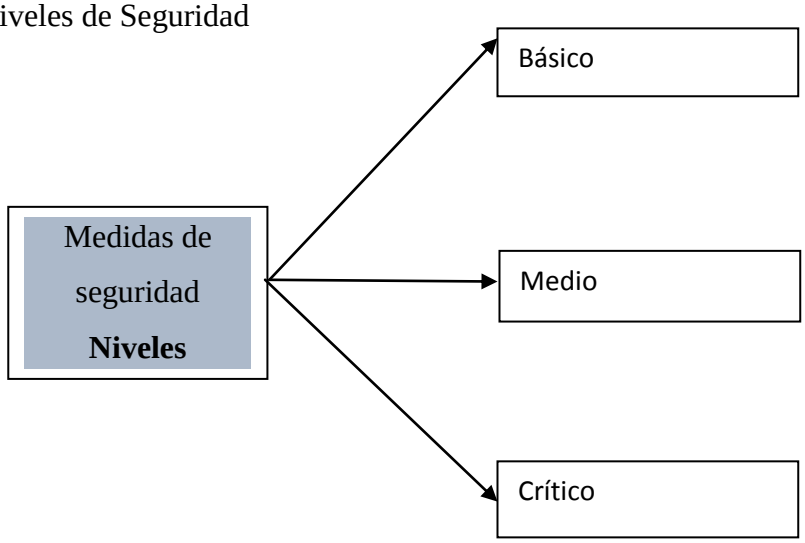
Por lo tanto, es necesario proteger la información contra la modificación sin autorización. Incluye no solo la que está almacenada directamente en los sistemas de cómputos sino que también se deben considerar elementos menos obvios como back ups, documentación, registros de contabilidad del sistema, tráfico de una red entre otros. Según la norma ISO/IEC 27000:2013 Integridad significa: "Propiedad de salvaguardar la exactitud y estado completo de los activos de información".

“Al recolectar, registrar, usar o transmitir datos personales, el responsable del archivo o banco de datos del caso se halla obligado, por imperativo legal, a cumplir las reglas de la buena práctica registral y a actuar, en todas sus operaciones con datos de forma de no violar la privacidad, los intereses y los derechos del interesado, ni generar un riesgo para la seguridad del Estado. Tiene esta misma obligación la persona que, como empresa independiente, actúa en nombre del mismo” (Carranza Torres, 2001, p.75).

La autoridad de control de la ley, la DNPDP, en ejercicio de su atribución de dictar normas y procedimientos técnicos relativos al tratamiento y condiciones de seguridad de las bases de datos, estableció disposiciones sobre este tema, entre las más destacadas:

La **Disposición 11/2006 es aquella** en la que se establece diferentes niveles de seguridad, para el tratamiento y conservación de los datos personales contenidos en archivos, registros, bancos y bases de datos públicos no estatales y privados.

Niveles de Seguridad



Se establecen tres niveles de seguridad: Básico, Medio y Critico, conforme la naturaleza de la información tratada. Para cada uno de los niveles se prevén distintas medidas de seguridad, establecidas teniendo en cuenta la mayor o menor necesidad de garantizar la confidencialidad e integridad de la información contenida en el banco de datos respectivo; la calidad de los datos y los riesgos a que están expuestos, así como también el mayor o menor impacto que tendría en las personas el hecho de que la información registrada en los archivos no reúna las condiciones de integridad y confiabilidad debidas.

Otra disposición de importancia que estableció la DNPDP es la **Disposición 09/2008,** en la cual se aprueba un modelo de documento de seguridad de datos personales y otros temas con referencia a la anterior Disposición 11/2006.

En la mencionada Disposición 09/2008 se estableció que los archivos, registros, bases y bancos de datos personales debían disponer de un "Documento de Seguridad de Datos Personales", en el que se especifica la normativa de seguridad aplicable. Para facilitar la implementación del referido documento y la puesta en funcionamiento de medidas técnicas que garanticen la seguridad y confidencialidad en el tratamiento de datos personales, es el mismo órgano de control quien establece un Modelo de Documento de Seguridad que contenga lineamientos indispensables considerados mínimos que permitan a los obligados diseñar un instrumento que se adecue a las necesidades de su organización y cumpla con las normas dictadas en la materia.

Artículo 10 - Deber de confidencialidad

En el **artículo 10** se legisla sobre el deber de confidencialidad de los datos personales. La Confidencialidad hace referencia a que los datos personales no puedan estar disponibles o ser descubiertos por personas, entidades o procesos no autorizados. En otras palabras, es la capacidad del sistema que realiza el tratamiento de datos personales, de evitar que personas no autorizadas puedan acceder a los mismos, a los recursos y de lo que se considere de importancia para asegurar que nadie pueda leer, copiar, descubrir o modificar datos personales sin autorización. Como así también, se evita la interceptación de comunicaciones o mensajes entre personas, entidades u otros.

“La obligación de mantener en secreto los datos que se registran alcanza no sólo al responsable de dicho banco, registro o archivo, sino también a cualquier persona que llegue a conocer de los mismos, por intervenir en su tratamiento. Esta obligación, que la ley inscribe dentro del género del secreto profesional, es de naturaleza personal, por lo que subsiste incluso luego de la extinción de la relación laboral o de género análogo por la cual hubiese conocido los mismos” (Carranza Torres, 2001, p.76).

Según la norma ISO/IEC 27000:2013 la confidencialidad es la: "Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados".

Como se observa el tema de la confidencialidad es muy importante, por ello se desarrollan mecanismos para la salvaguardia de la confidencialidad y seguridad de los datos personales y así se establecen medidas adecuadas para resguardarlos -teniendo en cuenta el estado del arte-, no obstante, se puede decir que no existe un único mecanismo capaz de proveer todos los servicios, pero muchos de ellos hacen uso de técnicas criptográficas:

1- Cifrado: garantiza que la información sea no inteligible para individuos, entidades o procesos no autorizados. Consiste en transformar un texto en claro –o texto plano– mediante un proceso de cifrado en un texto cifrado, gracias a una información secreta o clave de cifrado. Se utilizan criptosistemas simétricos como así también criptosistemas asimétricos.

2- Intercambio de autenticación: corrobora que una entidad, ya sea origen o destino de la información, es la deseada. Se debe ser cuidadoso a la hora de diseñar estos protocolos, ya que suele haber ataques para desbaratarlos.

3- El uso de técnicas de control de acceso a los sistemas: esfuerzo para que sólo aquellos usuarios autorizados accedan a los recursos del sistema o a la red, como por ejemplo: tarjetas inteligentes, huellas dactilares, retina del ojo, métodos clásicos basados en contraseñas entre otros.

4- Integridad de datos: mecanismo que implica el cifrado de una cadena comprimida de datos a transmitir, llamada generalmente valor de comprobación de integridad. Este mensaje se envía al receptor junto con los datos ordinarios. El receptor repite la compresión y el cifrado posterior de los datos y compara el resultado obtenido con el que le llega, para verificar que los datos no han sido modificados.

5- Tráfico de relleno: consiste en enviar tráfico espurio junto con los datos legítimos o válidos para que el atacante no sepa si se está enviando información ni qué cantidad de datos útiles se están transmitiendo. (Gozaíni, 2011)

Artículo 25: Prestación de servicios informatizados de datos personales

Y, en el **artículo 25** de la Ley Nº 25326 y su decreto reglamentario se introduce la figura del "encargado del tratamiento", para el caso del procesamiento de datos por cuenta de terceros, el cual no debe tratar los datos a su arbitrio, sino que se establecen obligaciones especiales, ya que tanto la ley como el decreto hacen referencia al "contrato de servicios" que vincula al encargado del tratamiento con el responsable o usuario. Entonces, el encargado de tratamiento: "es aquél que presta servicios de procesamiento de datos por encargo del responsable de una base de datos".

Se considera que se trata de una de las definiciones más importantes de la ley, ya que permite dar una idea del campo de aplicación y de amplitud del texto legislativo y de los contextos y situaciones en que el responsable del tratamiento debe ajustarse a los preceptos de la ley 25326. (Palazzi, 2004)

El tratamiento de datos personales por cuenta de terceros, especializados en prestarlos de manera profesional y eficiente es de gran utilidad para las organizaciones empresarias, debido a que les permite ahorrar costos en actualización de *software*, *hardware* y licencias entre otros.

También, cabe aclarar que "transferir", "ceder" o "transmitir" bases de datos para el tratamiento de los datos personales a un tercero, no implica transferir la propiedad de las bases de datos en cuestión, sino que se trataría de una cesión (artículo 11) para que se realice el tratamiento por un tercero o cesionario –se trata de otra excepción al artículo 11- y que debe cumplir con lo establecido en el artículo 25 y su reglamentación. Ésta última establece que los contratos de servicios de tratamiento de datos personales deberán contener los niveles de seguridad previstos en la Ley Nº 25326, el decreto reglamentario y las normas que dicte la Dirección Nacional de Protección de Datos Personales (DNPDP), como así también se deberá observar las obligaciones que surgen de los artículos 9 (Seguridad de los datos) y 10 (Deber de confidencialidad) de la mencionada ley.

Por lo tanto, en el caso de procesamiento de datos personales por cuenta de terceros, la ley dispone que el tercero proveedor de tales servicios deberá:

a) abstenerse de aplicar o utilizar los datos con un fin distinto al que figure en el contrato de servicios, ni cederlos a otras personas, ni aun para su conservación.
b) destruir los datos personales una vez cumplida la prestación contractual,
c) cumplir con las medidas de seguridad y confidencialidad establecidas en la ley en análisis.

Todo lo mencionado anteriormente deberá constar en un contrato escrito entre el responsable del banco de datos personales y el proveedor de los servicios de tratamiento de datos personales –tercero–. Y cabe distinguir dos situaciones:

- Cuando el prestador de los servicios de tratamiento de datos personales se encuentra en Argentina (y los datos son tratados en Argentina), debe aplicarse nuestra legislación vigente, la misma tiene carácter "de orden público".

- Cuando el prestador de los servicios de tratamiento de datos personales se encuentra fuera de Argentina cabe distinguir dos supuestos, según sea el país donde dicho tratamiento sea realizado:

a) países que "proporcionen niveles de protección adecuados de los datos personales" y

b) países que no.

En este último caso en el que el prestador de servicios se encuentra fuera de Argentina, se trata de transferencia internacional–, que ya fue tratado al comienzo de este punto.

Generalmente, la seguridad ha estado presente en los contratos informáticos, a través del establecimiento de cláusulas de confidencialidad y protección de datos de carácter personal. Pero los nuevos modelos de servicio en tecnologías informáticas requieren de una mayor especificación y nivel de detalle en materia de seguridad en la confección de los contratos por lo que requieren de una gran participación de los responsables de las áreas de seguridad respectivas.

Precisamente, llevando la cuestión del tratamiento y transferencia de datos personales al contexto de la nube, se puede advertir que no es fácil controlar, como responsable del tratamiento de los datos, que el proveedor de servicios de las llamadas *cloud computing* o computación en la nube–o tercero– cumpla con las obligaciones previstas por la ley, su decreto reglamentario y las resoluciones de la DNPDP. Razón por la cual es

necesario el establecimiento de cláusulas bien claras y específicas en el contrato de prestación de servicios que constituye un modo de dejar bien establecido las facultades y obligaciones de las partes intervinientes en el mismo. Motivo por el cual, en el próximo capítulo, se hará un estudio detallado de lo que se recomienda en los contratos de prestación de servicios informatizados de datos personales (o contrato de externalización –*outsoucing*–) en entornos c*loud computing,* con lo que se estaría cumpliendo con el artículo 25 inciso 1, al cual se delimita el presente TFG.

En muchas ocasiones la información que se prevé que debe poseer el responsable del tratamiento de los datos, en muchos casos, no la posee. Porque en el caso de encontrarnos en un nivel de servicio de las llamadas *cloud computing* o computación en la nube donde el ejecutor del tratamiento o procesamiento pone las condiciones de seguridad y privacidad de manera previa y unilateral, por lo que el responsable del tratamiento de los datos personales tiene menos posibilidades de controlar, en el caso de una cesión, que se cumpla con la normativa correspondiente.

Por ello, en este tipo de servicio –*cloud computing* o computación en la nube–, el énfasis se debe colocar en la seguridad y confidencialidad de los datos personales, los cuales merecen gran atención y cuidado.

La seguridad es un tema clave. Pero también lo es, la posibilidad de monitorear el uso que el proveedor del servicio hace de los datos del cliente y del cumplimiento del resto de las clausulas establecidas en el contrato, tema que se abordara más adelante.

Los datos que se almacenan en los entornos llamados *cloud computing* suelen residir en equipamiento compartido por múltiples clientes. Por ello, las organizaciones que gestionan datos personales en la nube deben preocuparse por la forma en que se accede a estos datos y garantizar que los mismos estén almacenados de forma segura. Otra cuestión importante, los datos deben ser protegidos cuando se encuentran en tránsito como en descanso. Asimismo, el acceso a los datos debe ser estrictamente controlado. Por ello, generalmente se pacta que el proveedor respetará la normativa sobre privacidad y seguridad de los datos, que se le impone a su cliente. De este modo, ambos quedan iguales, con similares deberes. Es una tranquilidad, pero que no resulta suficiente.

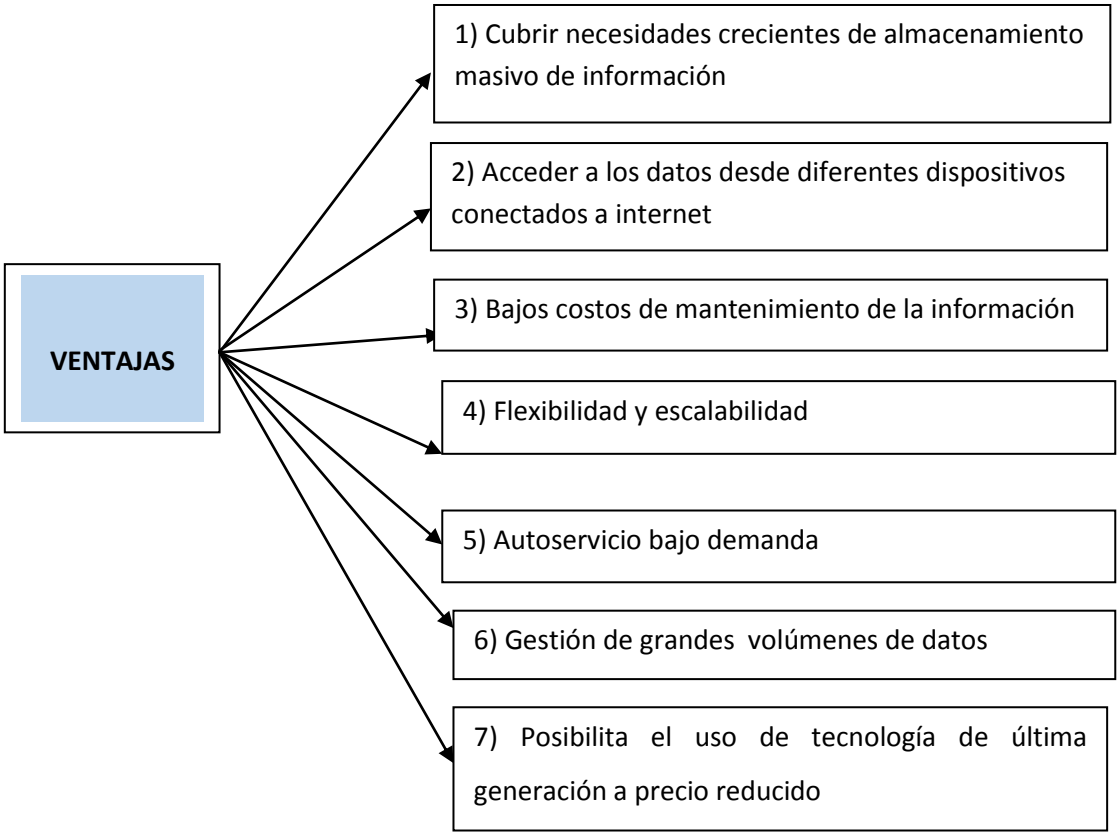
4.2- Ventajas y riesgos del almacenamiento de los datos personales en las llamadas "*cloud computing*" o computación en la nube[34]

El uso de los servicios de computación en la nube ofrece un gran número de ventajas pero presenta también, como no podía ser de otra manera, riesgos que deben afrontarse con una adecuada elección del prestador. Para lo cual debe analizarse que las condiciones de prestación tengan en cuenta los elementos que permitan que el tratamiento de los datos se realice sin merma de garantías que le son aplicables. Y debe observarse especial atención a no contratar servicios prestados en la nube que no cumplan o reúnan los requisitos establecidos por la legislación vigente.

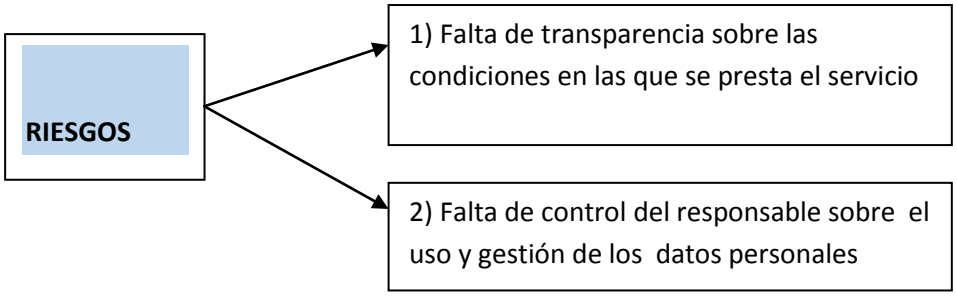
Para lo cual es necesario que el responsable de los datos estudie en detalle qué parte o partes de los tratamientos que realiza son factibles de ser transferidos a servicios de computación en la nube considerando no sólo los beneficios, sino de igual modo los potenciales riesgos que se van a asumir.

Así, se mencionan algunas de las ventajas y riesgos del almacenamiento de los datos personales en las llamadas "*cloud computing*" o computación en la nube:

[34] Se tendrá en cuenta guías de la agencia española de protección de datos, su página web (http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf)



En lo referente a los riesgos se considera que se los puede agrupar en dos grandes categorías:



1) Falta de transparencia sobre las condiciones en las que se presta el servicio

Es, justamente, el prestador el que conoce todos los detalles del servicio que ofrece. Por lo cual es necesario conocer el qué, quién, cómo y dónde se efectúa el tratamiento de los datos que se proporcionan al proveedor para la prestación del servicio acordado. Si él mismo no da la respectiva información, entonces el responsable de los datos no podrá

tener en claro cuestiones relevantes como la ubicación de los datos, la existencia de subencargados, los controles de acceso a la información o las medidas de seguridad.

De este modo, se le dificulta al responsable la posibilidad de poder evaluar los riesgos y así establecer los controles adecuados.

2) Falta de control del responsable sobre el uso y gestión de los datos personales por parte de los agentes implicados en el servicio

Por las particularidades del modelo de tratamiento de los datos en la nube, la falta de control del responsable se evidencia en casos como: a) dificultades para conocer en todo momento la ubicación de los datos, b) dificultades a la hora de disponer de los datos en poder del proveedor o de poder disponer de los mismos en un formato válido e interoperable c) la ausencia de control efectivo cuando se define los elementos sustantivos del tratamiento de los datos en lo referente a salvaguardas técnicas y organizativas.

Entonces, se observa que es necesario ser precavido en las cuestiones referentes al almacenamiento o tratamiento de los datos personales en las *"cloud computing*" o computación en la nube y dejar establecido en los contratos de este tipo de prestación todas las clausulas necesarias a fin de cumplir con la normativa de la ley 25326, su decreto reglamentario y las directivas de la DNPDP para no tener que lamentar luego la falta de recaudos.

4.3- Cuestiones relevantes del almacenamiento de los datos personales en las llamadas *"cloud computing"* o computación en la nube

4.3.1 Aspectos jurídicos

Se pueden considerar como transcendentes los siguientes aspectos jurídicos:

1) La puesta a disposición de los datos personales al proveedor de servicios constituye tratamiento de datos por un tercero, que puede implicar una cesión no consentida de datos.

2) La deslocalización de los servicios puede dar lugar a transferencias internacionales de datos no autorizadas.

3) La gestión de servicios en la nube puede llegar a provocar que el usuario pierda el control de la gestión de seguridad (integridad y confidencialidad de los datos)

4) Impone la necesidad de un mayor control de los contratos de prestación de servicios, donde se especifique en forma clara y precisa las obligaciones y derechos de las partes intervinientes en los mismos.

5) Importancia de las auditorías legales en las áreas tecnológicas de las empresas:

a. Licencias de software y documentación de equipos

b. Garantía del fabricante

c. Contratos de desarrollo con terceros

d. Registros de propiedad de marcas

e. Política de protección de bases de datos

f. Control del debido uso de los recursos tecnológicos por parte del personal (consiste en contar con los mecanismos para poder determinar qué es lo que sucede en el sistema, qué es lo que hace cada uno de los usuarios y los tiempos y fechas de dichas acciones).

4.3.2 Lista de verificación a la hora de contratar el servicio de *cloud computing*

1) ¿Se cumple con los niveles de seguridad de datos personales? (protección de datos personales)
2) ¿Existe posibilidad de subcontratar servicios? (outsourcing –identificación de todos los terceros que intervengan–se debe prestar atención en los subcontratistas)
3) ¿Qué proceso se efectuará en caso de pérdida de datos personales para su recuperación?

4) ¿Dónde se llevara a cabo el procesamiento de datos? (ubicación de los datos)

5) ¿Existen medidas de encriptación de los datos en tránsito, almacenada, back up y recupero de los datos? (por alguna clasificación formulada por la Ley 25326, es necesario recurrir a medidas especiales, todo ello debe estar previsto en el contrato)

6) ¿Existen medidas de seguridad que prevean protocolos de recuperación por desastres?

7) ¿Cómo y qué auditorias se podrían realizar tanto las estatales como las privadas?

8) ¿Existen límites de responsabilidad por parte del proveedor de *"cloud computing*? ¿Cuáles, son negociables?

9) ¿Legislación y jurisdicción aplicable en caso de los proveedores extranjeros?

10) ¿Qué garantías post contractuales brindan para el retorno íntegro y ordenado de los datos personales?

Conclusión

El poder de Internet y el aumento de las capacidades de cómputo como así también el progreso de nuevas tecnologías, hacen que los riesgos de intromisiones en la privacidad y los derechos fundamentales de los individuos sean mayores.
En la actualidad, se puede decir que hablar de *cloud computing* es hablar de Internet, un entorno en el que los datos se encuentran en constante movimiento a través de las fronteras, por lo que se necesita de la fijación de protecciones jurídicas y técnicas centradas en los datos en lugar de protecciones centradas en un territorio, ya que los datos son elementos que no son estáticos.

Por lo cual es necesario e imprescindible que las garantías de seguridad, confidencialidad, cesión, prestación de servicios informatizados por terceros y transferencia internacional entre otros, referidos a datos personales en un contrato de prestación de servicios *cloud computing*, deben ser bien específicos y detallados.

Entonces, resulta imprescindible delimitar contractualmente criterios concretos para así poder determinar la responsabilidad del proveedor de servicios *cloud* que trata los datos personales, ante eventuales incidentes que vulneren la seguridad, transmisión, integridad de los datos. Esto, debido a que el derecho debe tratar de dar respuesta a los nuevos problemas e interrogantes que surgen desde el entorno de computación en la nube, con cierta independencia de donde sucede el almacenamiento o el tratamiento de los datos personales, ya que en el espacio virtual este criterio no aporta valor.
Las garantías mencionadas deben, como mínimo, cumplir con la normativa aplicable. Asimismo, estas garantías deben gestionarse y establecerse contractualmente. Motivo por el cual, este tema será abordado en el próximo capítulo con mayor detalle.

Capítulo 5 El contrato de prestación de servicios tercerizados en entornos *cloud computing*

Introducción

"El avance de las nuevas tecnologías implica una constante inquietud para el análisis de la inserción de la informática en el ámbito jurídico. La discusión recién ha comenzado y mientras continúe este proceso global, es sin duda, uno de los temas fundamentales, la protección jurídica de los derechos individuales, a la luz de los avances tecnológicos" (Manili, 2010, p.3).

Se puede decir que todas las actividades humanas de una u otra forma están vinculadas al mundo de la informática y las nuevas tecnologías, entre las cuales ocupa un lugar destacado el derecho. Y también, se puede decir que prácticamente, ninguna rama del derecho ha quedado al margen de su influencia.

Así, en el vasto campo de las relaciones de las nuevas tecnologías –y que decir de la *cloud computing*– con el derecho cobra especial importancia el referido a la contratación.

El carácter específico de los contratos informáticos requieren en consecuencia un tratamiento jurídico especial que responda a las particularidades del mercado internacional de las nuevas tecnologías, a la especificidad de su objeto y de los intereses en juego para la empresa, Estado u organizaciones privadas y estatales**.**

Entonces, se propone en este TFG analizar algunos aspectos de las relaciones contractuales que rodean la gestión y servicios de los proveedores de servicios c*loud computing*, debido a su importancia creciente en la moderna contratación. Ya que se considera que si bien se aplican los principios generales de la contratación informática, también se hace necesario detectar, enunciar y dar respuesta a las particularidades de los procesos de externalización de los servicios *cloud computing.*

El *cloud computing* se diferencia del modelo de outsourcing TIC tradicional, en que en éste último existe una computación autónoma e independiente, el contratante –o responsable de los datos– puede saber en todo momento donde están alojados los datos y qué recursos se comparten con terceros, si es que se comparten, y los datos están

vinculados a una infraestructura determinada. En la nube o *cloud*, el servicio se desvincula de la infraestructura y el responsable de los datos no tiene en absoluto transparencia de los recursos que le están dando servicio en cada momento.

Entonces, este tipo de contrato es específico y complejo, debido al objeto y a la asimetría de la información de las partes intervinientes en el mismo. Estas cuestiones deberán atenderse adecuadamente al negociar y redactar las clausulas y anexos de un contrato de externalización –outsoucing– de los servicios c*loud computing.* Es así que se repiensan características propias de la etapa precontractual, la cuestiones referidas al software y al hardware de los sistemas, la problemática de los datos personales almacenados en bancos de datos de las organizaciones intervinientes en el contrato y su adecuada y necesaria protección, las cuestiones no menores de confidencialidad y seguridad, la problemática de la localización, los asuntos vinculados a recursos humanos afectados en la operación, la evaluación de estándares de servicio como así también las normas de calidad internacionales, entre otras cuestiones de importancia relevante. Todo lo enunciado deja ver una necesaria y nueva modalidad de contratos informáticos.

Ya que con la misma surgen muchos interrogantes legales, todos ellos de gran importancia. No obstante en este TFG se tratará de hacer un aporte en el análisis detallado del inciso 1 del artículo 25 -Prestación de servicios informatizados de datos personales- debido a que es de gran relevancia el contrato celebrado entre los proveedores de servicios en la nube y los responsables del banco de datos, considerándose en especial B2B (*Business to Business*), esto es, contratación entre empresas o personas jurídicas.

Luego de haber analizado y consultado fuente doctrinaria, llego a la conclusión de que lo más importante es que si o si se debe recurrir a la norma establecida en el artículo 25 de la citada Ley 25326, que es la que determina las condiciones en que se deben desenvolver las prestaciones de servicios informatizados de datos personales, con lo que se tratará de dar una respuesta lo más detallada posible referente a esta novedosa modalidad de contratos.

Al decir de Granero, *"Cloud computing* genera un apasionante desafío al campo legal y, por lo tanto, va a ser necesario en un futuro contar con políticas eficaces para garantizar los derechos a quienes se sirvan del sistema" y más adelante agrega el Dr. Granero "Sera necesario, por parte de los asesores legales, realizar un profundo análisis de los documentos contractuales que se celebren en la utilización de estos servicios para asegurar los derechos de los usuarios (protección de datos, propiedad intelectual, ley aplicable, juez competente)" (Barnitzke-Corrales-Forgó, 2012, p.12).

5.1 El contrato de prestación de servicios de Cloud Computing[35]

Se puede afirmar que existe una brecha entre la normativa vigente que regula la actividad de TICs y la realidad normada y, además en este fenómeno inédito para nuestra sociedad que sitúa a los doctrinarios, legisladores y juristas en la encrucijada de conocerlo, aprehenderlo y luego regularlo.

Como así también, se considera que la nueva riqueza de las naciones está constituida por el know how o recurso estratégico de la información, ya que en la actualidad se produce información en masa del mismo modo que los países industrializados fabricaban automóviles en masa. De modo que este caudal de información que hoy constituye fuente de riqueza, necesita de un marco jurídico que lo contenga y establezca reglas de juego claras. (Alterini, 2003)

Por ello corresponde resaltar que la legislación –leyes, resoluciones, directivas y otros– relacionada con la informática y las telecomunicaciones que las empresas deben cumplir no se redactaron pensando en el *cloud computing* y, también, es posible que los auditores u otros asesores externos con los que colabora o trabaja la empresa no estén familiarizados con *el cloud computing* en general o con algún servicio en la nube en particular.

Como un modo de recordar lo que se ha dado en conceptuar técnicamente como computación en la nube o su designación original en inglés *cloud computing*, se

[35] Se tendrá en cuenta el artículo "Cloud Computing: Aspectos jurídicos clave para la contratación de estos servicios" de la Revista Española de Relaciones Internacionales. Núm. 4. ISSN 1989-6565

entiende como un procedimiento que permite ofertar y prestar servicios a través de Internet, se trata de un servicio al que se puede acceder sin necesidad de contar con conocimientos especiales de ninguna naturaleza.
Se considera que el diseño del *cloud computing* es básicamente un espejo de la arquitectura de Internet, una red de comunicaciones que se extiende por la tierra, en la que los datos cruzan las fronteras jurisdiccionales millones de veces en cada segundo.

El manejo de Internet resulta una tarea delicada y compleja. Se necesita de los prestadores de servicios de Internet (ISPs-sigla en ingles), quienes cumplen una función fundamental en la prestación y el funcionamiento de esta red de comunicación. Se puede distinguir generalmente tres grupos de prestadores de servicios de Internet:

1- los Operadores de Redes y Proveedores de Acceso: los operadores mantienen el funcionamiento de la red y son los que permiten conectarse;

2- los prestadores de Servicios de Almacenamiento de Datos: ofrecen el soporte físico de los sitios Web y permiten interactuar;

3- los Proveedores de Servicios de Búsqueda y Enlaces: motores de búsqueda, son los que permiten navegar y encontrar lo que se necesita.

Como se observa todos estos integrantes de los tres grupos de ISPs, actúan en conjunto cuando un usuario utiliza y se conecta a Internet.
Es así, que en la actualidad se nos presenta lo que se conoce como *cloud computing* o computación en la nube que sin conocer nada respecto de "su existencia", se ha introducido en nuestras vidas mediante la transmisión o propagación de servicios de todo tipo a través de Internet, conmoviendo las estructuras tradicionales de la sociedad: organizaciones de toda índole, empresas, organismos públicos y privados, en fin en toda nuestra actividad humana cotidiana.
En este marco informático actual provisto por las tecnologías de la información, uno de los servicios más desarrollados es justamente, lo que se conoce como *cloud computing* o computación en la nube, tal vez su gran difusión se deba a que se trata de una estructura de distintas tecnologías de información que al asociarse a la proliferación de

comunicaciones de calidad a precios accesible, hizo factible la desmaterialización de un conjunto cada vez mayor de tecnologías y aplicaciones.
Se puede decir que más allá de las ventajas y desventajas, fortalezas y riesgos de lo que se ha dado en llamar como *cloud computing*, ésta es una realidad tecnológica y las ofertas de esta modalidad de servicio están al orden del día. El inconveniente principal se encuentra justamente en **la necesaria delegación en un tercero (**la prestación de servicios informatizados de datos personales o tercerización de servicios), especialista en el manejo de esta tecnología, del control de la seguridad (artículo 9) y confidencialidad o confiabilidad (artículo 10) de los datos.

Cabe aclarar que en lo que se refiere a la regulación del *cloud computing* o computación en la nube en nuestro derecho argentino, la misma no está legislada expresamente en la normativa nacional, por lo que se debe hacer jugar las reglas de los artículos 25, en especial, y en particular el 9 y 10 que se ocupa del tratamiento de la seguridad y la confiabilidad informática, como ya se mencionó anteriormente.

También, cabe subrayar que se debe tener en cuenta que en lo concerniente al usuario titular de los datos personales le quedan como resguardo jurídico todas las acciones que el derecho le ha otorgado para asegurarle el ejercicio del control sobre sus datos personales.

5.2 Consideraciones doctrinarias sobre el artículo 25 de la ley 25326

El artículo 25 de la ley 25326 fija específicamente el marco en el cual debe desenvolverse la prestación de servicios informatizados de datos personales de terceros. Se puede decir que la especificidad en la regulación está dada por las particularidades propias de la informática, como por la gran relevancia que posee la relación contractual que une a las partes.

En los contratos de prestación de servicios de procesamiento de datos, una de las partes hace entrega a la otra de un caudal de datos, con la finalidad de que ésta realice sobre los mismos determinadas operaciones que pueden ser, solo a modo de ejemplo: ordenación, actualización (altas-bajas-modificaciones), disociación, clasificación u otros, recibiendo por ello generalmente una retribución. (Carranza Torres, 2001)

“La complejidad de los sistemas de tratamiento de información y las posibilidades que ofrece el adelanto tecnológico, sumado a la posibilidad de disminuir los costos de reemplazo constante de tecnología ha provocado que gran cantidad de empresas adviertan la conveniencia de confiar buena parte de sus tareas informáticas a terceros especializados en prestar de manera profesional y eficiente servicios de gestión y tratamiento de datos” (Palazzi, 2004, p. 162).

Al referirse al artículo 25 de la ley 25326 expresa Gils Carbó (2001) “El encargado de tratamiento es sometido a las mismas reglas que debe observar el titular de un registro, presentándose la particularidad de que la cesión de datos por parte de quien requiere el servicio a quien lo presta, no exige el consentimiento del titular de los datos, porque no reviste propiamente la calidad de tercero al obrar por cuenta del otro” (p. 133).

Es por esta razón que quien encargó el tratamiento, no está relevado de su responsabilidad por las infracciones que pudiese cometer el prestador de servicio, ya que se trataría de un supuesto de culpa in *eligendo* (culpa en la elección) (Gils Carbó, 2001).

“La norma contempla el supuesto de “tercerización” de la operación de tratamiento de datos, es la que se configura cuando en virtud de una relación contractual estas últimas son desarrolladas por personas distintas de los responsables o usuarios de los bancos de datos, registros o archivos” (Basterra, 2008, p. 473).

La mayoría de la doctrina considera el supuesto del artículo 25 inc. 1 (Ley 25326) como “tercerización” de servicios de tratamiento, denominación que considero acertada para este tipo de relación contractual, puesto que la tercerización en el ámbito empresarial y más específicamente en el sector informático es de uso frecuente, como por ejemplo la que es llevada a cabo a través de las “consultoras” que son las encargadas de incorporar y contratar profesionales especializados en TICs para que luego éstos sean enviados a prestar servicios en las empresas.

Los contratos de prestación de servicios de tratamiento de datos personales deben cumplir con la normativa vigente en nuestro país. La cual establece que la realización de

tratamientos por encargo debe estar regulada por un contrato que vincule al encargado del tratamiento –o procesamiento– con el responsable o usuario del tratamiento.

Por lo que corresponde al cliente de los servicios de *cloud computing* comprender cuáles son las exigencias de cumplimiento normativo que implica la prestación de un determinado servicio a través del modelo nube, procurar un reparto de responsabilidades equitativo entre el proveedor del servicio en la nube y el cliente y así dar cumplimiento al marco normativo.

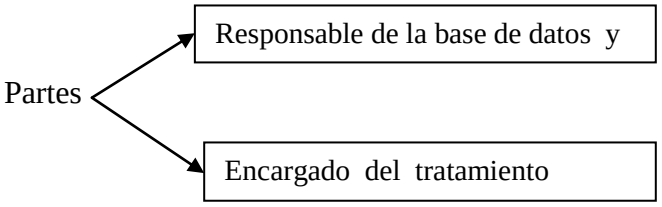
Por lo que resulta necesario e imprescindible que los departamentos jurídicos y de tecnología de las empresas clientes deberán implicarse y trabajar "codo con codo" durante el establecimiento de los Contratos de Acuerdos de Nivel de Servicios (generalmente detalladas en los denominados *SLAs* –por su sigla en inglés correspondientes al término *Service Level Agreement*–), y de las obligaciones contractuales, con el objeto de fijar qué requisitos de seguridad se pueden solicitar y alcanzar contractualmente mediante el establecimiento de métricas, normas de calidad internacionales y estándares adecuados.

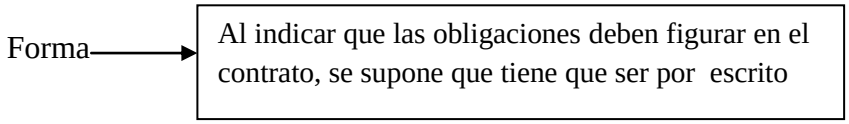
Se puede decir que la contratación de los servicios *cloud* se puede realizar en todos los niveles, tanto como por parte de personas físicas en calidad de consumidores, como por parte de las administraciones gubernamentales y entre personas jurídicas.

En este trabajo se analizará la prestación de servicios entre empresas de las relaciones denominadas B2B (*Business to Business*, en inglés), esto es, contratación entre empresas o personas jurídicas.

Es de imaginar que la prestación de servicios *cloud* a empresas se articula generalmente a través de un elemento básico y fundamental: la firma de un contrato entre las partes.

El contenido del contrato sintéticamente puede expresarse:





Algunos de los deberes del encargado del tratamiento

1) Deber de respeto a la finalidad del tratamiento
2) Deber de respeto a las instrucciones impartidas por el responsable
3) Imposibilidad de ceder los datos a terceros
4) Deber de no conservar los datos más allá de lo necesario
5) Deber de confidencialidad
6) Deber de seguridad

Es de gran importancia la redacción de un muy buen contrato de prestación de servicios en la nube, al respecto citaré opiniones vertidas por organismos de la Unión Europea; quienes ponen énfasis en la redacción de un contrato escrito que establezca en forma clara y precisa las etapas del contrato como así también las responsabilidades que genera para cada una de las partes.

Recomendaciones legales[36]: La mayoría de las cuestiones legales asociadas a la computación en la nube se suele resolver durante la evaluación -cuando se comparan los distintos proveedores- o en la negociación del contrato. El caso más común de computación en la nube es la selección de los distintos contratos que ofrece el mercado (evaluación de contratos), en contraste con la negociación del contrato. No obstante, podría haber oportunidades para que clientes potenciales de servicios en nube seleccionaran proveedores con contratos negociables.

[36] ENISA, Cloud-computing - Beneficios, riesgos y recomendaciones para la seguridad de la información, 2009, p. 6, disponible en https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish

Se recomienda revisar detenidamente las cláusulas estándar del contrato, debido a la naturaleza de la computación en la nube. Las partes del contrato deben prestar especial atención a sus derechos y obligaciones en lo que respecta a las notificaciones de incumplimiento de los requisitos de seguridad, transferencias de datos, confidencialidad, cambio de control y acceso a los datos por parte de las fuerzas policiales. Es por ello que en el capitulo anterior y en el presente se hace mención y estudio a todas estas cuestiones.

Al respecto en "Guías de Seguridad de áreas críticas en Cloud Computing" de la Cloud Security Alliance[37], versión 3 se puede leer:

> Cuando los datos son transferidos a Cloud, la responsabilidad de su protección y seguridad sigue siendo, habitualmente, de quien los recaba o custodia, si bien bajo algunas circunstancias esta responsabilidad puede estar compartida con otros. Cuando se encarga a un tercero que aloje o trate estos datos, el custodio de los datos sigue respondiendo ante cualquier pérdida, daño o uso no autorizado de los datos. Es prudente, y en ocasiones obligatorio, que el custodio y el prestador de servicios de Cloud firmen un contrato por escrito que defina claramente las funciones y expectativas de las partes, y las responsabilidades que corresponden a cada una de ellas en relación con los datos en cuestión.

5.3 Características de los contratos *cloud computing*

Generalmente, los contratos utilizados para regular los servicios de *cloud computing* suelen ser:

- Contratos de adhesión en los que los proveedores de servicios en la nube imponen sus propias condiciones, con el consiguiente riesgo para la parte contratante ya que no posee capacidad de negociación respecto del reparto de responsabilidad en la seguridad de la conservación de los contenidos y la obligatoriedad del cumplimiento de normas en materia de datos personales. Lo ideal es que fuesen contratos específicamente negociados entre las partes, en todo caso debería regir el principio de libertad de forma.

[37] https://www.ismsforum.es/ficheros/descargas/guia-csa1354629608.pdf

- Obligaciones de medios y no de resultados, se configura como una obligación de medio y no de resultado porque se refiere a un contrato de prestación de servicios. Debiera en este caso como excepción, establecerse una serie de obligaciones de resultado por los riesgos a que se enfrenta la empresa y por relevancia de las funcionalidades que la interesada está delegando en el prestador de servicios *cloud*.

- "Externalización" o "*outsourcing*", se estima que el concepto de externalización de los servicios no ofrece dudas respecto de su significado e implicaciones, pero, se considera que no está de más acudir a la definición concreta que de la expresión "*outsourcing* informático" hace el autor español Davara Rodríguez –en su obra "Manual de Derecho Informático"–, y conforme a la cual el mismo consiste en: "La cesión de la gestión de los sistemas de información de una entidad a un tercero que, especializado en esta área, se integra en la toma de decisiones y desarrollo de las aplicaciones y actividades propias de la referida gestión, con la finalidad de la optimización de los resultados de la misma, al tiempo que permite a la entidad el acceso a nuevas tecnologías y la utilización de recursos especializados de los que no dispone".

  La definición citada pareciera exceder el ámbito de los contratos de c*loud*, por incluir no sólo el almacenamiento de datos e información (así se entiende el c*loud* en sentido estricto) sino también la gestión de esa misma información mediante aplicaciones tecnológicas concretas, pero la realidad demuestra la frecuencia con la que el objeto de estos contratos supera el mero almacenamiento de información.

Antes de adentrarse en el contrato se recomienda obtener la mayor cantidad posible de información de los probables prestadores del servicio de *cloud computing*, tal como domicilios reales de los *Data Centers*, solvencia económica y financiera, antigüedad en el sector o rubro, cartera de clientes actuales y casos de éxito y fracaso, auditorías de calidad realizadas y certificaciones obtenidas y nivel de cumplimiento normativo como así también historial de litigios referidos al servicio que brindan.

5.4 Clausulas típicas de un contrato empresarial de servicios *cloud computing*

Se consideran clausulas típicas de un contrato empresarial de servicios *cloud computing*:

5.4.1 El contrato marco y sus anexos
5.4.2 Clausulas típicas

a) Identificación de las partes, expositivos, el objeto del contrato
b) Las obligaciones de las partes
c) Protección de datos de carácter personal
d) Otras cláusulas típicas
e) Cláusula de resolución del contrato

5.4.1 El contrato marco y sus anexos

Se puede decir que el contrato empresarial de servicios de entorno c*loud* se estructura en torno a dos partes fundamentales: de un lado, el propio contrato –denominado en muchas ocasiones contrato marco– que contendrá los aspectos de carácter general que regularán la relación entre las partes, y por el otro, los anexos que complementan a aquél con el detalle y especificaciones particulares que asegurarán la conveniencia y satisfacción de las necesidades de la empresa contratante.

Así, lo que en la práctica más habitual pase por esta división persigue simplificar la comprensión y organización del propio contrato. Entonces, los anexos deben contener aquellas consideraciones que resulten eminentemente técnicas sin que ello suponga que su contenido sea de importancia inferior a lo estipulado en el propio contrato marco.

Tal vez ocurre lo contrario, ya que con frecuencia el detalle del alcance de los servicios que deben ser prestados por la empresa de c*loud* queda contenido en un anexo, así como incluso el propio precio pactado entre las partes y generalmente desglosado con cada una de las prestaciones pactadas.

Habitualmente, también se acompaña como anexo al contrato el detalle de los procedimientos a seguir para los servicios de operación y mantenimiento a llevar a cabo por el prestador de servicios de *cloud*; este anexo, suele incluir, un reparto de responsabilidades entre las partes en el que queda establecido a cuál de ellas

corresponde la obligación de contratar determinados servicios de terceros: desde los servicios de un *call center* hasta la contratación de una plataforma de pago *online*. En lo referente a las cuestiones relacionadas con protección de datos de carácter personal, el detalle correspondiente a las medidas de seguridad a adoptar en cumplimiento de la normativa vigente al respecto suele constituir otro de los anexos típicos y de gran importancia de este tipo de contratos.

Cabe mencionar que resulta aconsejable que desde un punto de vista eminentemente práctico, y debido a la constante evolución de las funcionalidades de las tecnologías de la información y de las comunicaciones, en el contrato marco se establezcan aquellos mecanismos procedimentales que procuren que los anexos "técnicos" puedan renovarse durante toda la vigencia del contrato siempre que concurran el consentimiento de ambas partes y el de las personas designadas en cada parte, sin que el contrato marco deba ser también modificado.

5.4.2 Clausulas típicas

a) Identificación de las partes, motivos o expositivos, el objeto del contrato

El contrato de prestación de servicios de Cloud comenzará con la necesaria identificación de los contratantes (partes), donde se hará constar, no solo la identidad de los mismos y de sus representantes, sino también la actividad a la que cada una de las empresas se dedica.

La costumbre –rige en los contratos el principio de libertad de forma (art. 958 CCyC) – indica que seguidamente a la identificación de los contratantes, se encontrará por lo general la denominada parte expositiva. En ella, se enumeran con cierto nivel de detalle (sin ser excesiva) las necesidades de cada una de las partes –aquella que será beneficiaria de los servicios de *cloud*– y las posibilidades de satisfacer las mismas de que dispone la otra parte, –el prestador de los servicios de *cloud*–. Es conveniente incorporar motivos claros y concisos sobre las necesidades, razones e intenciones que llevan a las partes a formalizar el contrato en cuestión. Lo mencionado anteriormente es útil ante el potencial surgimiento de discrepancias en la interpretación de las cláusulas, ya que podrán resultar de utilidad y arrojar cierta luz respecto de la intención verdadera de los contratantes.

Las partes acuerdan mediante una declaración la firma del contrato en cuestión, cuyas condiciones habrán de sostenerse sobre la base de las cláusulas que, por lo general, se acompañan a continuación de los motivos.

Entre tales cláusulas existe una serie de ellas que son típicas, por ser recurrentes y fundamentales en la estructuración y conformación de las condiciones contratadas.

Una de las más importantes es la relativa al objeto del contrato, pues la misma colaborará a la correcta resolución de posibles controversias interpretativas y supondrá una contextualización del resto de cláusulas.

b) Las obligaciones de las partes

Tal vez, una de las cláusulas de mayor relevancia sea aquella que determina las obligaciones de cada una de las partes nacidas de la formalización del contrato (generalmente dividida en dos subcláusulas que contienen las obligaciones de cada una de las partes respectivamente). La identificación de las obligaciones de cada parte interviniente resulta fundamental, como así también la claridad de su redacción, pues la omisión de alguna de ellas, como la oscuridad de su redacción podría dar lugar o constituirá un claro germen de conflicto entre las partes.

También, resulta muy conveniente prever contractualmente la prohibición de cambios contractuales unilaterales, generalmente para evitar que el contratista realice modificaciones unilaterales en los términos del servicio y así evitar la cautividad del cliente.

Se debe mencionar que existe la posibilidad de que los proveedores de servicios externalicen parte de sus servicios a través de contratos de *outsourcing* y es muy importante que si ello ocurre se asegure y se identifique la cadena de responsabilidad a lo largo de los procesos y servicios para poder tener un control efectivo sobre los servicios que van a ser prestados. Con el fin de evitar vacíos de responsabilidad por daños causados por estas empresas subcontratadas es conveniente que se añadan cláusulas en los contratos de modo que los prestadores de servicios *cloud* con los que se contrata se responsabilicen de la actuación y cumplimiento de la normativa de las empresas subcontratadas.

Con respecto a la independencia de la ubicación física –muy usual en el *cloud computing*– sobre la que el propio cliente generalmente no tiene control, se puede y se debe pedir al prestador de servicios que contractualmente aporte informaciones específicas sobre el país, la región, o un determinado centro de datos.

Así también, resulta muy conveniente prever contractualmente las consecuencias que deben derivarse de la posibilidad de que, en la medida en que un mayor número de clientes compartan la infraestructura de la nube, se produzcan sobrecargas en los servidores y degradaciones en la calidad del servicio efectivamente ejecutado por los prestadores.

De modo adicional, y pese a que ello podría deducirse del contenido genérico del contrato, se puede establecer con claridad, si las obligaciones a las que quedan sujetas cada una de las partes son obligaciones de medio u obligaciones de resultado. Conviene aclarar y sería aconsejable que los contratos empresariales de prestación de servicios de *outsourcing de cloud* pueden llegar a generar en el prestador de los mismos, obligaciones de resultado y no simplemente de medio. Estas obligaciones de resultado deben quedar debidamente delimitadas y abordadas mediante los Acuerdos de Nivel de Servicio.

c) Protección de datos de carácter personal

La relevancia que cobra este aspecto en los contratos empresariales de servicios de *cloud* genera, como consecuencia, que deba siempre incluirse una cláusula que contemple la regulación contractual de la protección de datos de carácter personal.

Sin perjuicio del modo en que se articule el flujo de datos en cada caso particular, por lo general, una prestación de servicios de *cloud* entre empresas supondrá un supuesto de comunicación de datos a un tercero, lo que sería una cesión (artículo 11) de acuerdo a nuestra Ley 25326 o prestación de servicios informatizados de datos personales (artículo 25). O incluso podría tratarse de una transferencia internacional de datos personales (artículo 12) del mismo texto normativo.

En cualquier caso, la cláusula deberá identificar claramente al responsable del banco de datos en cuestión, así como quién actuará como encargado de su tratamiento. Por otra parte, y como se verá, las partes pueden incluir –y generalmente se configura como anexo– un detalle de las medidas de seguridad, integridad y confidencialidad a adoptar

de conformidad con lo establecido en la Ley 25326 y su Decreto reglamentario. Por lo que es recomendable que el proveedor posea certificaciones internacionales en lo que a seguridad de la información se refiere, por ejemplo la norma ISO 27001:2005 y posteriores.

Es necesario establecer una cláusula en la que se establecerán las condiciones en que el tratamiento de los datos tendrá lugar y la finalidad para la que se destinarán los mismos.
Las medidas a adoptar para su protección variarán en función del tipo de información que se comparte con el prestador de servicios. Puede ser que pase de encontrarnos tanto ante una transferencia de datos de carácter personal (por ejemplo, datos de los empleados transmitidos para la prestación de un servicio de recursos humanos o de elaboración de nóminas de empleados) como ante información constitutiva de secreto comercial de la compañía.
Se debe tener presente que este tipo de servicios se prestan a menudo valiéndose de un traslado de la información por parte del prestador de servicios de *cloud,* a servidores que pudieran estar ubicados en el extranjero. Es un aspecto altamente importante que debe evaluarse en la forma adecuada, en el momento de negociación del contrato de servicios de *cloud,* pues en función de las condiciones en que tal movimiento internacional de datos se produzca –transferencia internacional–, las implicaciones para las partes son muy diversas.
Se puede decir que, la vía contractual supone la mejor de las garantías para la tranquilidad de las empresas que externalizan el almacenamiento de sus secretos comerciales. Por ello es de gran importancia la necesidad de establecer con claridad las medidas de seguridad, confidencialidad y el alcance de las mismas, encaminadas a impedir tanto el acceso de terceros no autorizados a la información de la compañía –incluido personal del propio prestador de servicios de *cloud*–.

d) Otras cláusulas típicas

Existen otros aspectos que también deben tenerse presentes a la hora de elaborar un contrato de prestación empresarial de servicios de *cloud*.
Entre otros aspectos:

d.1) Cláusulas de propiedad intelectual e industrial

Estas cláusulas son fundamentales en este tipo de acuerdos, ya que resulta evidente que, los medios necesarios para prestar los servicios objeto del contrato (sistemas informáticos, aplicaciones, sistemas de gestión y otros) se encuentran protegidos por derechos de este tipo.

Por la complejidad de los servicios de *cloud* pueden resultar necesarios que el beneficiario de los mismos instale en sus propios equipos o materiales algún tipo de programa que permita un fácil acceso a la información y datos que el prestador de servicios está alojando en sus servidores. Entonces, resulta crucial que las partes expresamente reconozcan en el propio contrato que todo uso que con motivo de la materialización de lo dispuesto en el mismo hubieran de hacer de este tipo de obras será, en todo caso, autorizado por el titular de sus derechos o, en su caso, que serán las propias partes (cada una respecto de los elementos que aporte) las titulares de los mismos. Así, el beneficiario de los servicios de *cloud* deberá tener presente (y así se tiene por costumbre hacer constar en el contrato) que el hecho de que el prestador de servicios de *cloud* le permita hacer uso de este tipo de elementos, no supone más que eso: un licenciamiento de uso de un software en el que deben observarse pautas claras de comportamiento tanto en relación con su mantenimiento evolutivo como correctivo.

d.2) Anexo eminentemente técnico

Como así también debe incluirse una cláusula o un anexo eminentemente técnico relativo a lo siguiente:

a) medidas de encriptación o cifrado de los datos en tránsito, almacenados, *backup* y recupero de los datos. Es recomendable que el proveedor explicite por contrato la técnica de cifrado que utiliza. En el caso de que se negase a brindar dicha información, por ejemplo por considerarla confidencial, se puede recurrir a un tercero de acreditado prestigio para auditar las medidas de seguridad.

b) procesos, protocolos y políticas de *backup* y recuperación datos personales

Se considera altamente recomendable exigir al proveedor del servicio que exponga su política de *backup* y plan de recuperación de datos ante desastres en caso de incidentes graves. Dicho plan establece los procedimientos necesarios para volver a la operación

normal de un negocio, lo antes posible y con la menor perdida de datos luego de un desastre natural o humano.

c) garantías post contractuales que se brinden para el retorno íntegro y ordenado de los datos personales

Por cualquiera de los motivos expuestos en el apartado "Cláusula de resolución del contrato" o cualquier otro, será necesaria la transferencia de los datos por parte del proveedor hacia el cliente. El contrato deberá contar con una cláusula en la cual se consigne lo siguiente:

- Medio y formato en el cual se transferirán los datos.
- Plazos.
- Asignación de costos para cada una de las partes.

Una vez traspasados los datos al contratante, el prestador del servicio y todas las terceras partes que hayan estado involucradas deberán destruir todo rastro de los mismos, incluyendo cualquier copia de seguridad que posean.

Entonces, todo contrato empresarial de prestación de servicios *cloud* contiene –en su cláusula correspondiente cuando no en un Anexo específico– los términos más estrictos para lograr la máxima protección para la información de mayor relevancia. Si bien es cierto que las cláusulas con este contenido están considerablemente estandarizadas, su revisión y ajuste por las partes resulta altamente recomendable.

d.3) Cláusula sobre jurisdicción

Cabe mencionar la importancia de incluir una cláusula relativa a jurisdicción y ley aplicable. Al respecto, las partes podrán acordar la renuncia expresa a cualquier fuero que pudiera corresponderles para la resolución de cuantas controversias pudieran surgir en relación con el contenido del contrato y su correcto cumplimiento.

Cláusula típica por excelencia de prácticamente cualquier tipo de contrato, cobra especial relevancia en los contratos de prestación de servicios de *cloud*.

En este punto se hace referencia a las diversas alternativas disponibles para la resolución de conflictos fuera del ámbito jurisdiccional. Así, se deben destacar los beneficios de la utilización del mecanismo del arbitraje o de la mediación –muy especialmente en el sector tecnológico–, que son por todos conocidos: mayor rapidez,

eficacia y, sobre todo, tener la posibilidad de acudir a profesionales con profundos conocimientos técnicos en la materia de que se trate.

Ya que un procedimiento judicial en el que concurren elementos internacionales –como suele ser común en el ámbito tecnológico del *cloud*– puede extenderse años, resulta extremadamente complejo, y, además, significa costos elevados. Por lo que aquellos contratos mercantiles más modernos y avanzados prevean la posibilidad de optar por alguno de los citados tres métodos más comunes para la resolución de conflictos sin llegar a juicio: la negociación, la mediación y el arbitraje.

Cabe resaltar que, en el ámbito internacional el arbitraje se está imponiendo como un método de resolución de conflictos realmente efectivo para las empresas independientemente de su tamaño, pues además de ofrecer una serie de ventajas respecto a la vía judicial ordinaria, puede evitar a las partes el sometimiento a jurisdicciones extranjeras que puedan ser totalmente desconocidas. Por ello es que la fase de negociación de los contratos se presente como el momento ideal para fijar el compromiso de sometimiento a un sistema arbitral ante una posible controversia futura. Ya que es en ese momento que, las partes están imbuidas por una firme voluntad de acuerdo y un sentido de mutua ganancia.

d.4) Cláusula sobre la reserva de la posibilidad de auditar

Las empresas clientes deben reservarse en los contratos la posibilidad de auditar, en el marco de un adecuado proceso de *due diligence* –análisis que brinda una visión global de la empresa–, las infraestructuras informáticas y los procesos de gestión de la seguridad –normas, medidas, estándares– de la información implantados por el proveedor.

La cláusula contractual referente a la reserva del derecho a auditar debe obtenerse siempre que sea posible, muy especialmente cuando se utiliza un proveedor en la nube para un servicio ante el cual el cliente mantiene importantes responsabilidades de cumplimiento normativo. Por lo que deberá detallarse en el contrato de servicios la forma y periodicidad en la cual se realizarán las auditorías al prestador y la manera en la cual se comunicarán los resultados.

d.5) Cláusula sobre propiedad de los datos

Cuando se establece un contrato con un proveedor de servicios *cloud* se debe definir de forma clara y precisa los derechos sobre los datos para poder crear un primer marco de confianza. El contrato de servicios *cloud* debe establecer de forma clara que la organización mantiene la propiedad de todos sus datos, asimismo debe asegurar que el proveedor no adquiere derechos o licencias a través de los acuerdos para usar los datos en su propio beneficio.

Generalmente, existen controversias importantes en torno a los términos ambiguos que utilizan los proveedores de servicios *cloud* en sus políticas de privacidad y propiedad de los datos.

e) Cláusula de resolución del contrato

Se deberán estipular las posibles causas de resolución del contrato con el prestador del servicio *cloud* tales como:

- Finalización por vencimiento del plazo de vigencia
- Mutuo acuerdo
- Falta de pago
- Violación de las condiciones del servicio
- En caso de incumplimiento por alguna de las partes de las obligaciones asumidas en el contrato, la otra parte podrá dar por resuelto enteramente el mismo, sin preaviso ni indemnización de clase alguna, siendo suficiente la comunicación de tal rescisión a la parte contraria.
- Quiebre financiero del prestador

Se considera necesario analizar las causas una por una y elaborar detalladamente la forma de actuar en cada una de las situaciones mencionadas. Algo común en todas ellas, será la devolución de la información por parte del prestador al cliente que se hará teniendo en cuenta lo expuesto en "garantías post contractuales que se brinden para el retorno íntegro y ordenado de los datos personales" del presente trabajo.

5. 5 La importancia de las cláusulas contractuales tipo de la Decisión 2010/87/UE

En febrero de 2010, la Comisión Europea adoptó la Decisión 2010/87/UE, y con ella, un conjunto de artículos contractuales tipo para transferencias entre responsables y encargados del tratamiento, respectivamente, con el objeto de responder a la expansión de actividades de tratamiento y en particular, la aparición de nuevos modelos de negocio para el tratamiento internacional de datos personales.

A la luz de esta Decisión, cuando las transmisiones de datos se realicen entre un responsable de datos y un encargado del procesamiento, se considera que reúnen las garantías adecuadas aquellos contratos que contengan las cláusulas contractuales tipo aprobadas.

De ese conjunto de cláusulas tipo, resultan especialmente relevantes en los entornos *cloud computing* las siguientes:

- Ley aplicable: En lo relativo a la protección de datos, se aplicará la legislación del Estado Miembro en el que está establecido el exportador de datos.
- Responsabilidad: El importador (proveedor de servicios *cloud)* será responsable subsidiario de los daños y perjuicios a los titulares de los datos como resultado del incumplimiento de las obligaciones contenidas en las cláusulas.
- Seguridad: El importador de datos (proveedor de servicios *cloud*) ofrecerá garantías suficientes en lo que respecta a las medidas de seguridad técnicas y organizativas específicas detalladas y especificadas en un anexo al contrato.
- Auditoría: el importador de datos (proveedor de servicios *cloud*) ofrecerá a petición del exportador de datos sus instalaciones de tratamiento de datos para que se lleve a cabo la auditoría de las actividades de procesamiento cubiertas por las cláusulas. Esta será realizada por el exportador de datos o por un organismo de inspección, compuesto por miembros independientes con las calificaciones profesionales necesarias y sujetos a la confidencialidad, seleccionado por el exportador de datos y, cuando corresponda, de conformidad con la autoridad de control.
-Subcontrataciones: La subcontratación de las operaciones de procesamiento requerirán de dos requisitos: a) previo consentimiento por escrito del exportador de datos y b) que el subencargado del tratamiento que se contrata garantice que proporcionará, al menos, el mismo nivel de protección de los datos personales y los derechos de los interesados que el importador de datos proporciona en virtud de las cláusulas.

-Jurisdicción competente: El importador se somete a la jurisdicción del exportador de datos (cliente de *cloud*) a los efectos de cualquier reclamación por daños y perjuicios por parte de los titulares de los datos.
-Deber de cooperación: Las partes acuerdan que la autoridad de control está facultada para auditar al importador (proveedor de *cloud*), o a cualquier subencargado, en la misma medida y condiciones en que lo haría respecto del exportador de datos conforme a la legislación de protección de datos aplicable.

Expresan que al estar estas cláusulas disponibles para importadores ubicados en todo el mundo, se continúa de esta manera la transición europea desde un modelo basado únicamente en protección territorial, hacia un modelo basado en compromisos contractuales.

5.6 Perspectiva futura de las *"cloud computing"*

Resulta evidente que la demanda de las llamadas *"cloud computing"* –computación en la nube– aumentará de forma muy significativa en los próximos años, ya que, como se ha expresado en el presente trabajo son indudables las numerosas ventajas técnicas y económicas que brinda este servicio. Apostar al *"cloud computing"* les permite a las empresas asignar sus recursos propios de modo eficiente, enfocándose en su actividad principal y delegando la gestión informática en el tercero proveedor del servicio, lo que a su vez les permite ahorrar dinero en inversión en tecnología y su constante actualización en software y hardware como así también en licencias y desarrollos de infraestructura.

Por ejemplo, cuando una empresa contrata un servicio en la nube, le entrega los datos de terceros a un proveedor. A partir de allí, pierde el control y los cuidados de su seguridad. Ya que implica transferencia de información fuera del control de la empresa que contrata el servicio. Y se debe tener presente que el procesamiento y almacenaje de esa información puede estar fuera de la Argentina.

En el paper "Problemas legales de la *Cloud Computing*"[38] el Dr. Granero expresa que: "se podría definir *"cloud computing*" como el sistema informático que ofrece la migración o la externalización de los equipos de computación y de los programas o las funciones de procesamiento de datos a un prestatario de servicios que otorga su almacenamiento a través de los servidores diseminadas sin identificación necesaria de su ubicación, por un precio determinado o determinable."

Y más adelante expresa: Es evidente que el servicio de *"cloud computing*" merece la atención de todos los sectores –privados y de los gobiernos nacionales– pues como toda tecnología de punta es siempre bienvenida, pero lo cierto es que también genera un verdadero desafío al campo legal, y por lo tanto, serán necesarias políticas eficaces para proporcionar certeza legal a los "servicios computacionales en la nube" y a sus usuarios.

En la actualidad, se puede decir que, más allá de los beneficios técnicos y económicos que brinda este servicio, las empresas todavía poseen desconfianza y dudas a la hora de delegar en un tercero el procesamiento y/o almacenamiento, por las cuestiones no menores del control, la confidencialidad y seguridad de los datos. Y también se debe tener presente que si algo sale mal, sigue siendo la empresa la responsable frente al titular de la información cedida.

Otro punto de gran importancia, es que la evidente adaptación y crecimiento del uso de la computación en la nube, ha producido, produce y se incrementará aún más, en un futuro cercano, la atención no querida de sectores potencialmente dañinos. Se puede afirmar que hasta hace muy poco tiempo, una organización empresarial, financiera o bancaria era un objetivo buscado y preferido de ataque cibernético, en la actualidad el objetivo preferido de ataque es un proveedor de servicios en la nube, lo que incrementa muchísimo el impacto, el daño y el valor del ataque.

Por lo que comparto lo que expresa, el Dr. Granero en lo que respecta a la tarea que los abogados tengamos por delante, particularmente por el necesario asesoramiento que debemos efectuar a los potenciales contratantes, poniendo de resalto los potenciales

[38] Granero, H. *"Problemas legales de la Cloud Computing".* El Dial. 12/10/2010 [Papers-elDial.com] Adquisición y Consulta: 28 junio 2017.

riesgos legales que el servicio puede generar a la luz de la normativa vigente en cada área (salud, bancaria, etc), lo que se deberá ver plasmado en los contratos que se celebren en cada caso, cuyas cláusulas, debidamente analizadas y consensuadas entre las partes exceden los escuetos lineamientos de una simple orden de compra.
El respaldo de la garantía de diligencia en el obrar de los responsables de las empresas contratantes está en juego, y su juzgamiento no será precisamente "en la nube" sino en nuestros Tribunales.

5.7 Consideraciones que podrían afectar la protección de los datos personales en ámbitos *cloud computing*[39]

Hay temas que tienen relación con los datos personales y que configuran un desafío a nivel legislativo, ya que se presentan lagunas en la legislación nacional y a nivel internacional ha sido tratados de manera exigua. A continuación se hará mención de los siguientes:

1) Datos personales encriptados o codificados
2) Datos personales fragmentados
3) Datos derivados o titularidad sobre los nuevos datos generados

5.7.1 Datos personales encriptados o codificados

Se sabe que los datos personales se definen como información de cualquier tipo relacionada con personas que pueden ser determinadas, mediante un esfuerzo razonable, por el solo hecho de conocerse esa información.

El *cloud computing*, como una arquitectura distribuida, implica un mayor tráfico de datos en comparación con las arquitecturas tradicionales. Motivo por el cual se aconseja la protección de los datos personales contra la filtración de datos o accesos no autorizados, en especial cuando los mismos están en tránsito. También se aplica para el

[39]ENISA, Cloud-computing - Beneficios, riesgos y recomendaciones para la seguridad de la información, 2009, disponible en https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish

almacenamiento, para impedir que otros tomen conocimiento del contenido de los datos. Por ello se aconseja que los datos se protejan a través de la codificación o más precisamente a través de métodos o algoritmos criptográficos.

Aquí, cabe aclarar que la Teoría de la información dice que todos los criptosistemas son quebrables y la teoría de la complejidad informa si ello será posible dentro de un minuto o antes de la muerte térmica del universo, aun contando con recursos computacionales astronómicos. Las tecnologías de la información y las comunicaciones tal como las conocemos en la actualidad no hubieran sido posibles sin la teoría matemática que desarrollo Claude Shannon. Ya que sus investigaciones tuvieron gran impacto en diversas áreas del conocimiento, pero fue en la industria de las telecomunicaciones donde sus teorías tuvieron más relevancia.

La codificación o el encriptado es el proceso de transformar información -datos personales- (texto) a través de un algoritmo para hacerlo ilegible (texto cifrado) para todos salvo aquellas personas autorizadas que posean la clave para descifrarlo.

Los algoritmos criptográficos o de codificación se desarrollaban basados en la suposición de que era poco probable identificar al multiplicador de un número primo grande, con una cantidad razonable de tiempo y dinero. No obstante, la potencia de las computadoras ha aumentado considerablemente, y su costo para utilizarlas ha bajado, precisamente con el surgimiento del *cloud computing*, entonces los datos personales pueden estar cada vez más expuestos a riesgos.

Sobre el tema Gils Carbó (2001) expresa: "La criptografía es la ciencia que se ocupa de proteger la información mediante la utilización de algoritmos matemáticos que transforman los documentos en un extremo y realizan el proceso inverso en el otro extremo, de modo que solo pueden ser descifrados por quien está munido del código o password establecido" (p. 102).

Así, desde un punto de vista técnico, los datos personales codificados o encriptados son (o corresponderían ser) datos seguros, ya que se impide que terceros puedan tomar conocimiento de los mismos. Y desde un punto de vista legal los datos personales codificados o encriptados aun no ha sido tan debatido en la doctrina legal.

Pareciera que no habría motivos razonables para negarle protección a los datos personales codificados o encriptados, caso contrario se encontrarían en peores situaciones o condiciones legales que los datos personales no codificados o encriptados. Entonces, los datos personales codificados o encriptados necesitan el mismo nivel de resguardo -seguridad- que los datos personales en su versión texto. (Barnitzke-Corrales-Forgó, 2012)

5.7.2 Datos personales fragmentados

El uso de sistemas de almacenamiento distribuidos en la nube o *cloud computing* puede llevar a una significativa fragmentación de los datos personales. Con la expresión de fragmentación de datos personales se hace referencia a que los archivos o banco de datos (y en consecuencia, los datos que éstos contienen) almacenados en sistemas de almacenamiento distribuidos pueden extenderse sobre distintas ubicaciones y centros de datos. Entonces, además del almacenamiento distribuido, los datos están fragmentados: los archivos o banco de datos grandes están segmentados en distintas partes. Luego, estas distintas partes se distribuyen y almacenan en distintas ubicaciones y hasta en distintos centros de datos.

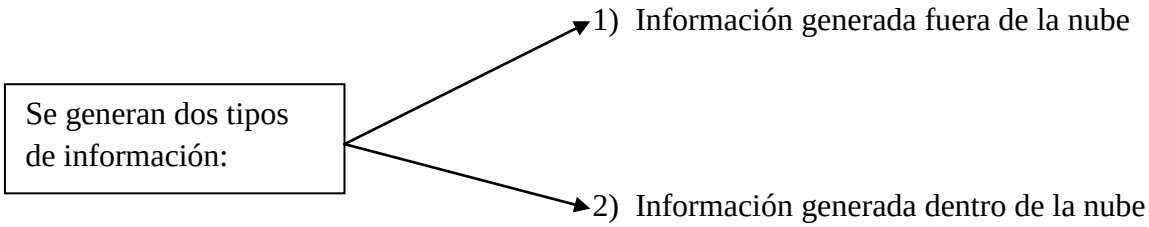
> No obstante, cuando se leen los datos dentro de un sistema de almacenamiento distribuido, el sistema (es decir los programas) tiene que unir distintos fragmentos relacionados de archivos o bases de datos para poder entregar los datos correctos a un cliente o a otro proveedor de nube que solicita la información. Entonces, los datos fragmentados en un sistema de almacenamiento distribuido es información sobre personas determinables. Por lo que se tendría que considerar como datos personales, ya que es posible combinar los fragmentos o segmentos e identificar a la persona.

5.7.3 Datos derivados o titularidad sobre los nuevos datos generados

La eventual titularidad de los datos generados con la implementación del servicio de computación en la nube genera todo un debate acerca de a quien corresponde los derechos de propiedad (o titularidad) sobre los nuevos datos.

La propiedad de los datos hace referencia tanto a la posesión y a la responsabilidad de la información, lo cual implica el control sobre esa información.

El *cloud computing* permite mediante la ejecución de procesos o tratamiento de datos que se genere nueva información, que puede ser de propiedad tanto del cliente como de los proveedores de servicio *cloud.* Ello, debido a la forma compleja en que los datos se almacenan y comparten en la nube, se puede decir que:



1) Información generada fuera de la nube

La mayoría de la información que se instala o sitúa en la nube ya tiene propietarios preestablecidos, entonces, tiene sentido pensar que tales propietarios querrían seguir siéndolo.

Desde el punto de vista legal, recomiendan que se debe prestar atención a: 1) derecho contractual 2) secretos comerciales 3) propiedad intelectual. Por lo que es aconsejable para evitar confusiones que se exprese en forma clara, precisa a través de las cláusulas y condiciones de un contrato.

Asimismo, "los contratos tendrán un rol importante al establecer los derechos de propiedad a través de las condiciones de servicio" (Barnitzke-Corrales-Forgó, 2012, p.141).

2) Información generada dentro de la nube

Esta temática es la más compleja, debido a que una de las características del *cloud computing* es justamente, permitir procesamientos que generan nueva información que se instala en la nube, que puede ser de propiedad tanto de los clientes como de los proveedores de servicio *cloud.*

Se observa que el principal problema de establecer derechos de propiedad en entornos *cloud computing* son los llamados derechos derivados, como por ejemplo los nuevos datos obtenidos de procesamientos como *datamining* –mineria de datos–.

Se recomienda que se debe tener en cuenta dos cuestiones: a) ley aplicable al contrato y b) competencia correspondiente (es decir la jurisdicción aplicable)

a) ley aplicable al contrato: cuando hay un contrato escrito, las partes intervinientes suelen determinar mediante una clausula especifica la jurisdicción que regirá la relación contractual.

b) competencia correspondiente: cuando no hay clausula específica que rija la jurisdicción contractual.

5.8 Consideraciones acerca de la necesidad de modificación de la Ley Nº 25326

Hace diecisiete años desde la sanción de la Ley Nº 25326, es de conocimiento público que para todo lo que es informática, tecnología y telecomunicaciones es muchísimo tiempo, en esa época el concepto de *cloud computing* aun no existía en el mundo.
Como se ha analizado, nuestra legislación no trae una figura que se aplique específicamente para el *"cloud computing"*, por ende se debe recurrir a los artículos 25, 9, 10, 11 y 12 entre otros, de la ley 25326 y a las especificaciones de esos artículos que prevé el decreto reglamentario 1558/01. Como así también a las disposiciones de la Dirección Nacional de Protección de Datos Personales para lograr un marco legal que permita proteger los datos alojados y tratados en la nube.
Considero que se debe reflexionar acerca de una reforma integral de la ley 25326, para así considerar si son suficientes las previsiones existentes en materia de protección de datos personales considerándolo en el contexto mundial de la tecnología y su impetuoso avance.

Por todo lo mencionado, me inclino a favor de una reforma de la ley 25326 o de un nuevo marco regulatorio que contemple las llamadas *"cloud computing"* o computación en la nube, pero con lineamientos generales y no con demasiadas especificaciones para no quedar desactualizadas en un plazo breve. La misma debiera estar redactada por

equipos interdisciplinarios de abogados, ingenieros o licenciados de carreras afines a la informática y a las telecomunicaciones para así lograr una buena ley que tienda a la seguridad jurídica de los datos personales de los ciudadanos, y esté acorde a los tiempos que nos toca vivir. Además, considero que hay que prestar atención al tema de tratamiento de datos por parte de terceros pero que quede determinado de manera taxativa.

Cabe recordar que la protección de datos y la protección de la privacidad son temas de agenda mundial, debido a que tienen que ver con problemas de vigilancia –lucha contra el terrorismo y crimen organizado– y de comercio–en gran medida comercio electrónico– y su cambio de reglas va a impactar también en Argentina, debido a que estamos en presencia de un mundo cada vez más globalizado y también, recordando que la tecnología siempre supera en velocidad al derecho.

Porque como expresara Alberdi[40] "Sembrad fuera de la estación oportuna: no veréis nacer el trigo. Dejad que el metal ablandado por el fuego recupere, con la frialdad, su dureza ordinaria: el martillo dará golpes impotentes. Hay siempre una hora dada en que la palabra humana se hace carne. Cuando ha sonado esa hora, el que propone la palabra, orador o escritor, hace la ley. La ley no es suya en ese caso; es la obra de las cosas. Pero esa es la ley duradera, porque es la verdadera ley."

Y como también expresa Alberdi "Los progresos de su civilización pueden modificarla y mejorarla en el sentido de la perfección absoluta del gobierno libre, pero pactando siempre con los hechos y elementos de su complexión histórica, de que un pueblo no puede desprenderse, como el hombre no es libre de abandonar, por su voluntad, su color, su temperamento, su estatura, las condiciones de su organismo, que recibió al nacer, como herencia de sus padres".

[40] www.acaderc.org.ar/ediciones/publicaciones/2002/homenaje-a-juan...alberdi/

Conclusión

La técnica es, entonces, según Ortega, "la reforma que el hombre impone a la naturaleza en vista de la satisfacción de sus necesidades". Esta reforma de la naturaleza da lugar a la sobrenaturaleza: la *sobrenaturaleza de la técnica*.[41]

Y porque el hombre es originariamente deseo, sus necesidades son una invención; no coinciden con la naturaleza, sino que residen en la sobrenaturaleza en cuanta concreción de su capacidad técnica. Al tiempo que la exalta, no se cansa Ortega de advertir, con mirada premonitoria, sobre fundamentalismos que unos cincuenta años después de su muerte ponen en peligro al hombre que se inventa para ser. Dice, por ejemplo, que "la técnica, al aparecer por un lado como capacidad, en principio ilimitada, hace que al hombre, puesto a vivir de fe en la técnica y sólo en ella, se le vacíe la vida". Este hombre hueco –resignificación del hombre-masa de *La rebelión de las masas* – es incapaz de inventar su propia vida. "Sólo en una entidad donde la inteligencia funciona al servicio de la imaginación creadora de proyectos vitales, puede constituirse la capacidad técnica".

Entonces, cabe preguntarse que tipo de sociedad podría surgir como consecuencia de los adelantos tecnológicos de nuestros tiempos y de los del futuro. Sin lugar a dudas, se estará en presencia de una tensión permanente entre lo que nos posibilita la tecnología y lo que la ética aconseja, seguramente aquí debe entrar en juego la sujeción al orden ético –la decisión que se toma debe ser prudente y justa–.

Como se sabe, el derecho tiene un fin que es el bien común, por lo tanto debe existir un ordenamiento de esta tecnología, porque así como puede generar grandes avances, éstos pueden ser bien o mal usados.

[41] Citado por el Ing. Horacio Reggini en "Prudencia y técnica", La Nación del 22 de marzo de 2001.

Conclusión Final

El tema de este trabajo final de grado (TFG) tiene que ver no solo con la protección jurídica de los datos personales, sino también con la misma dignidad humana.

En una sociedad cada vez más relativizada en sus aspectos morales será más difícil detener los quehaceres habituales de un banco de datos con todo lo que ello implica. Así, es sabido que la globalización es una realidad sin regreso que, indudablemente se hará cada vez más intensa y al decir de Bidart Campos "la continuidad del fenómeno estatal que ya hoy ha entrado en intersección con la globalización nos mostrará adaptaciones y cambios, tensiones y conflictos, todo en el marco de un desafío por la supervivencia" (Bidart Campos, 2004, p.198). Por lo que se ha vuelto casi imposible que un país disponga de poder para evitar la penetración y circulación de medios, información, comunicación, en síntesis todo se ha vuelto extraterritorial, así como también en los ámbitos financieros, bancarios, comerciales, industriales y por supuesto que también en el mercado de consumo.

Es, en este contexto que se desarrolla el presente TFG y pretende ser un aporte al trabajo interdisciplinario que debe haber entre el Derecho y las Ciencias Informáticas–Tecnológicas. Por lo que en el capítulo 1 se aborda brevemente, la realidad tecnológica actual, en la que se observa que prácticamente en todas las empresas de cualquier servicio e industria cuentan con un departamento de sistemas, quienes tienen por finalidad obtener información necesaria para la toma de decisiones. Y con el crecimiento de dicho sector se han incrementado los costos asociados a telecomunicaciones, hardware, licencias de software, personal calificado, tercerización, entre otros. Como así también, la necesidad de contar con información actualizada en todo momento y desde cualquier dispositivo hace que se incremente la complejidad y los costos de hardware y desarrollo de software.

Así, en la actualidad se presenta una solución para ello, llamada *cloud computing*, que se consolida frente a otras. Por lo que se realiza una descripción de la misma, de sus niveles de servicio y formas de despliegue. Ya que es relevante entender cómo funciona este servicio para lograr comprender dónde se alojarán y tratarán los datos que se deben proteger.

Si bien es cierto que la *cloud computing* es una buena solución a nivel económico, técnico y funcional, puede también resultar un dolor de cabeza a nivel legal. Por lo cual en el capítulo 2, se realiza un marco de referencia de la legislación vigente en nuestro país sobre el tema planteado para este TFG. En base al relevamiento y análisis realizado sobre las actuales leyes de protección de datos personales, especialmente nuestra ley Nº 25.326, se logra así obtener un marco de referencia sobre el cual basar los acuerdos legales con los proveedores de c*loud computing* a la hora de contratar ese servicio por una organización, lo que se analiza con mayor detalle en el capítulo 5.

Mientras que en el capítulo 3 se enuncian y analizan brevemente los fallos considerados más relevantes por la mayoría de la doctrina en nuestro país. Luego, en los capítulos 4 y 5 se analiza con mayor profundidad la temática de la *cloud computing* o computación en la nube observando así que en nuestro país hay poco o casi nada de doctrina referente al tema mencionado. Motivo por el cual se tuvo que recurrir a trabajos o sugerencias de España, ya que nuestra ley 25326 se baso en la ley española.

Al analizarse la normativa vigente en la Argentina sobre la protección de datos personales, se establece cuales regulaciones son compatibles con el sistema del *cloud computing* y qué cuestiones quedan sin regular o es insuficiente la regulación. Para lo cual se trabaja especialmente con el concepto de la cesión de los datos, el consentimiento del titular, la seguridad, la confidencialidad, la transferencia internacional como así también la prestación de servicios informatizados de datos personales por terceros.

Y se concluye recomendando que es necesario su tratamiento legislativo ya sea modificando la ley 25326 o en una nueva ley pero teniendo presente que será necesario escuchar y analizar a sectores de la informática, telecomunicaciones, sociólogos y abogados, es decir un marco interdisciplinario que permita tener una visión más acertada de la *cloud computing* o computación en la nube para lograr una ley acorde a estos tiempos que corren. Pues es sabido que Internet y qué decir de la *cloud computing* presenta grandes desafíos a los juristas y gente del derecho, ya que al proyectarlas al campo jurídico deja en muchas ocasiones perplejos y balbuceantes a prestigiosos jueces y doctrinarios y ello tal vez se deba a que falta directrices en el campo normativo y jurisprudencial.

Por lo que se deben buscar soluciones a los problemas que las nuevas tecnologías generan –en este caso *cloud computing* o computación en la nube– ya que la esencia del hombre de leyes debe ser evaluar permanentemente la eficacia de las normas y construir líneas rectoras de las nuevas situaciones que se presentan. Por lo que en este TFG se trató de hacer un análisis lo más preciso posible de las cuestiones más relevantes a tener en cuenta en un contrato de prestación de servicios *cloud*, el cual seguramente presenta aspectos a ser mejorados al ser llevado a la práctica, que es lo que siempre acontece con todo aquello que involucra a la informática y a las nuevas tecnologías.

Se puede decir que todo lo que involucra a las *TICs* es un debate muy rico, de grandes alcances y por supuesto que también, es trabajoso. También cabe recordar que parte de la filosofía, el derecho y la sociología han anticipado observaciones a un mundo tecnológicamente desarrollado y democrático, y ya señalaron los grandes riesgos existentes en materia de concentración y control social.

Al decir de Mosset Iturraspe "está en los signos de los tiempos que nos tocan vivir que la persona humana sea objeto de detrimentos, menoscabos, ataques, al fin, que son fuente de perjuicios; empero, los medios empleados por los agentes son, ahora, acordes con los avances de la ciencia y de la técnica; se puede decir que más sofisticados o sutiles; y, a la vez, hieren o dañan aspectos del ser humano que antes permanecían ocultos o desconocidos" (Mosset Iturraspe, 2011, p. 199 y 200).

Y entre uno de los daños más importantes están aquellos que se causan a la persona a través de la manipulación de los datos personales, "que debiendo estar protegidos están desprotegidos y posibilitan así el avance sobre la dignidad, la privacidad, la reserva" (Mosset Iturraspe, 2011, p. 201).

Pareciera que se desconoce todo este bagaje cultural, como así también que la tendencia actual en la red, se orienta hacia la creación de grandes grupos que establecen alianzas que terminan guiando al "navegante" por caminos señalizados según conveniencias predeterminadas. Así mismo, es sabido que todo lo concerniente a la manipulación de datos personales y a su recolección es de gran interés para el conocimiento del mercado, y detrás de esta temática, están estas grandes empresas generalmente extranjeras, que se benefician y lucran grandemente con ello.

Observo y coincido con Mosset Iturraspe y Bidart Campos cuando se refieren al tema de la globalización y posmodernidad que transitamos y nos toca vivir, de la gran influencia empresaria sean multinacionales o transnacionales, las cuales influyen y hasta participan en las esferas políticas, jurídicas y culturales. Todo ello, para lograr en las decisiones de esos poderes un contenido o decisión que le resulte de su interés. Aquí cabe preguntarse hasta qué punto ese contenido o decisión es independiente y hasta qué punto ese contenido o decisión es influenciado, condicionado o si es simplemente una imposición. Del mismo modo cabe relacionarlo con el tema en tratamiento, toda regulación de los datos personales les influye y les perjudica actualmente o en un futuro cercano. Por ello se multiplican las voces y argumentos a favor de la libertad de comercio y de información como así mismo invocan la defensa de la ciencia informática.

Así el poder económico transnacional y extraterritorializado invade las jurisdicciones de los países con su pensamiento global especulativo, dando por resultado que unos pocos ricos sean cada vez más ricos y enviando así a pobres a ser cada vez más pobres, hasta quedar por debajo de las necesidades básicas insatisfechas. Se observa en este fenómeno dos caras: 1) una clase capitalista, que en definitiva opera como un contrapoder ante el poder de los estados y 2) un grandísimo conjunto de excluidos sociales, para los que seguramente no habrá muchas posibilidades de movilidad social ascendente. Y al decir de Borges "Ser pobre implica una más inmediata posesión de la realidad, un atropellar el gusto áspero de las cosas; conocimiento que parece faltar a los ricos como si todo les llegara filtrado" (Gentile, 2010, pág. 58).

Es en este marco, en el cual se debe legislar y no vacilar porque lo que se encuentra en juego es la seguridad jurídica de los datos personales y su regulación, temas que plantea el avance tecnológico, el cual no tiene precedentes en toda la historia de la humanidad. Estos nuevos desafíos en el campo del derecho, se deben a que produce o pueden llegar a producir una gama de daños y responsabilidades legales que no están previstos en las normas vigentes en nuestro país. Así, se plantean cuestiones entre otras como las siguientes: 1) - El concepto de "servicio peligroso" aplicable a la tecnología y la inversión de la carga de la prueba. 2)- La teoría del orden público tecnológico 3)- El principio precautorio deja de ser un concepto del derecho ambiental y se extiende al

ámbito de la tecnología - “principio precautorio”, que se traduce como la obligación de suspender o cancelar actividades que amenacen el medio ambiente pese a que no existan pruebas científicas suficientes que vinculen tales actividades con el deterioro de aquél–.

Sabido es que nunca habrá consenso absoluto, tampoco habrá unanimidad de pareceres para el tratamiento de este tipo de regulaciones o normativas, pues los intereses en juego son fuertes y poderosos y las grandes empresas no están dispuestas a claudicar. Si tenemos en cuenta que grandes empresas multinacionales manejan los datos personales, esto se convierte en un combo peligroso para los particulares por la evidente desproporción en las facultades que tienen los actores. Por lo que resulta imperioso que el Estado legisle y regule el tema, tutelando y protegiendo a la parte más débil dentro de la relación.

Estas regulaciones deben resguardar la privacidad, el consumo, la moral, el trato igualitario y no discriminatorio. Eso sí, presenta una cuestión difícil de regular ya que Internet crece y evoluciona rápidamente, y lo hace de manera caótica y a escala global, lo cual la hace resistente a las pretensiones normalizadoras de los sistemas jurídicos nacionales. Por lo que se sostiene la necesidad de sancionar normas que deben ser marcos regulatorios mínimos, como así también tratados internacionales o de carácter comunitario, que fijen de igual modo marcos regulatorios mínimos y comunes para su adaptabilidad a las naciones, y sean sobretodo capaz de mantener una flexibilidad permanente a los nuevos desafíos.

Nuestros representantes en el Congreso de la Nación deben tener presente el viejo adagio “lo mejor es enemigo de lo bueno” como así también que no se legisla “para la eternidad”, y sabiendo que es función primordial de las leyes poner fin a conflictos, actuales o potenciales.

En este estado de situación resulta evidente que no debe demorarse la palabra del Derecho del Estado en este tema, que como se observa en el desarrollo de este trabajo tiene mucho que ver con la dignidad, la privacidad, la confidencialidad, la seguridad y en definitiva con la realización plena del hombre en su estancia terrenal.

Bibliografía

Doctrina

- Alterini, J., (2003), *Prueba, Responsabilidad y Derecho Informático*, Buenos Aires Argentina: La Ley
- Altmark, D., (2006), *El contrato de outsourcing de sistemas de información*, Buenos Aires Argentina: LexisNexis
- Altmark, J., (2015), *Dossier: Habeas Data –Selección de Jurisprudencia y Doctrina*, Buenos Aires, Argentina: SAIJ
- Avalos E., Buteler A., Massimino L., (2014), *Derecho Administrativo*, Córdoba Argentina: Alveroni Ediciones
- Barnitzke-Corrales-Forgó, (2012), *Aspectos legales de la Computación en la Nube*, Buenos Aires Argentina: Editorial Albremática
- Basterra M., (2008), *Protección de datos personales*, Buenos Aires Argentina: Ediar
- Bidart Campos G. , (1997), *Manual de la Constitución Reformada* (Tomo 2), Buenos Aires Argentina: Ediar
- Bidart Campos G., (1998), *Manual de la Constitución Reformada*, Buenos Aires Argentina: Ediar
- Bidart Campos G., (2004), *La Constitución que dura*, Buenos Aires Argentina: Ediar
- Castells, M., (2005), "*La era Información" – Economía Sociedad y Cultura- La Sociedad Red* Vol. I, Buenos Aires, Argentina: Editorial Siglo XXI editores argentina S.A.
- Carranza Torres, L., (2001), *Habeas data: la protección jurídica de los datos personales*, Córdoba Argentina: Alveroni Ediciones
- Cifuentes, S., (1978), *Los derechos personalísimos*, Buenos Aires Argentina: Editorial Lerner
- Cifuentes, S., (2007), *El derecho a la vida privada – Tutela a la intimidad*- Buenos Aires Argentina: La Ley
- Cortina, A., (2000) *Ética de la empresa*. Madrid España: Ed. Trotta.

- Ekmekdjian M. y Pizzolo (H.), (1995), *Habeas Data. El derecho a la intimidad frente a la revolución informática,* Buenos Aires Argentina: Ediciones Depalma.
- Feldman, E., (2008), *El Pacto de San José de Costa Rica***,** Santa Fe Argentina: Rubinzal – Culzoni Editores
- Fernández Delpech, H., Poullet, Y. y Pérez Asinari, M. – Palazzi, P. (2009), D*erecho a la intimidad y Protección de datos personales,* Buenos Aires Argentina: Heliasta
- Gates, B., (1999*), "Los Negocios en la Era Digital",* Buenos Aires, Argentina: Editorial Sudamericana.
- Gelli, M., (2003), *Constitución de la Nación Argentina; comentada y concordada*, Buenos Aires Argentina: La Ley
- Gils Carbó, A. (2001), Régimen Legal de las Bases de Datos y Habeas Data, Buenos Aires Argentina: La Ley
- Gozaíni, O. (2003), *Habeas Data – Protección de Datos Personales,* Santa Fe, Argentina: Rubinzal – Culzoni Editores
- Gozaíni, O. (2011), *Derecho Procesal Constitucional - Habeas Data – Protección de Datos Personales*, Santa Fe, Argentina: Rubinzal – Culzoni Editores
- Granero, H., (2003), *El orden público tecnológico,* Buenos Aires Argentina: Educa
- Manili, P., (2010), *Tratado de Derecho Procesal Constitucional,* Buenos Aires Argentina: La Ley
- Masciotra, M. (2003), El hábeas data - la garantía polifuncional, La Plata (Buenos Aires), Argentina: Librería Editora Platense
- Molina Quiroga, E. y Luz Clara, B., (2011), *Derecho Informático,* Buenos Aires Argentina: La Ley
- Morello –Loñ, (2003), Lecturas de la Constitución, Buenos Aires, Argentina, Editorial Lexis Nexis.
- Mosset Iturraspe, J., (2011), *Derecho civil constitucional*, Santa Fe, Argentina: Rubinzal – Culzoni Editores
- Negroponte, N., (1995), *Ser digital*, Buenos Aires, Argentina: Atlántida

- Oyarzabal, M. (2007), Lecciones y Ensayos Nº 83, Buenos Aires Argentina: Facultad de Derecho –Universidad de Buenos Aires (U.B.A.)
- Padilla, M. (2001), *Bancos de datos y Acción de habeas data*, Buenos Aires Argentina: Abeledo-Perrot
- Palazzi, P. (2002), *La transmisión internacional de datos personales y la protección de la privacidad*, Buenos Aires Argentina: AD-HOC
- Palazzi, P. (2004), *La protección de los datos personales en la Argentina*, Buenos Aires Argentina: Errepar

- Papert, S., (1987), "*Desafío a la mente" Computadoras y Educación*, Buenos Aires, Argentina: Ediciones Galápago
- Pierini, A. – Lorences, V. – Tornabene, M., (2002), *Habeas Data – Derecho a la intimidad*, Buenos Aires Argentina: Editorial Universidad S.R.L.
- Puccinelli, O., (2004), *Protección de datos de carácter personal*, Buenos Aires Argentina: Editorial Astrea
- Quiroga Lavié, H., (2000), *La Constitución de la Nación Argentina comentada*, Buenos Aires, Argentina: Zavalía
- Rossati, Barra, García Lema, Masnatta, Paixao, Quiroga Lavié; (1994), *La reforma de la Constitución*, Buenos Aires, Argentina: Rubinzal – Culzoni Editores.
- Rosatti, H., (2010), *Tratado de Derecho Constitucional* - tomo1, Santa Fe, Argentina: Rubinzal – Culzoni Editores
- Sagüés, N., (2007), Manual de derecho constitucional, Buenos Aires Argentina: Editorial Astrea.
- SAIJ -Sistema Argentino de Información Jurídica-, (2015), *Dossier: Habeas Data*, Buenos Aires Argentina
- Stallings W., (2000), "*Comunicaciones y Redes de Computadores*", Madrid, España: Prentice Hall
- Uicich, R., (2009), *El derecho a la intimidad en Internet y en las comunicaciones electrónicas*, Buenos Aires Argentina: AD-HOC.
- Yuni J., – Urbano, C., (2003*), "Tecnicas para investigar y formular proyectos de investigación – Volumen I",* Córdoba, Argentina: Editorial Brujas.

Revistas

- Arcos Valcárcel de Caramelo, S. y Caramelo Díaz, G. (1998). "Datos personales, acerca de la protección de los datos en el ámbito informático", *Revista Plenario*, Asociación de Abogados de Buenos Aires (n° 43), 6-9.
- Hassemer, W. (1999). Oportunidades para la privacidad frente a las nuevas necesidades de control y las tecnologías de la información. *NDP*. Nº A, 97-120
- Palazzi, P. (1998). El hábeas data en el derecho argentino. *Revista de Derecho Informático - Alfa-Redi*- No. 004.
- Cifuentes, S. (2008). El Derecho a los Datos Personales y Habeas Data. *Revista Anales 53(46)*, 117-126.
- Toro, R. y Olivera, R. (2009). El derecho al olvido, matices y recepción legislativa, doctrinaria y jurisprudencial en el derecho patrio. *Revista Abeledo Perrot Córdoba.* Nº 3, 241-250.

Jurisprudencia

- *CSJN, (2012), Habeas Data*-Comunicaciones. Secretaría de Jurisprudencia, Buenos Aires Argentina. www.CSJN.gov.ar
- C.S.J.N."Ponzetti de Balbin c/Editorial Atlántida S.A", Fallos 306:1892(1984)
- C.S.J.N, "Urteaga, Facundo Raúl c/ Estado Nacional – Estado Mayor conjunto de las FF.AA. s/ amparo ley 16.986" Fallos 321:2767 (1998)
- C.S.J.N., r. p., r. D. c/ Estado Nacional – Secretaría de Inteligencia del Estado, Fallos: 334:445 (2011)
- C.S.J.N., "Halabi Ernesto c/ P.E.N**.** ley 25.873 Dto. 1563/04", Fallos: 331:2784, (2008)
- C.S.J.N., María Belén Rodríguez contra *Google Inc. s/* daños y perjuicios (2014)

Legislación

- Constitución de la Nación Argentina
- Declaración Universal de Derechos Humanos
- Convención Americana sobre Derechos Humanos llamada Pacto de San José de Costa Rica
- Código Civil y Comercial de la Nación
- Ley Nº 25326 (Habeas Data o Protección de Datos Personales) y su Decreto reglamentario Nº 1558/2001
- L.O.R.T.A.D. (Ley española de 1992)
- Disposición 11/2006 de la DNPDP
- Disposición 09/2008 de la DNPDP
- Disposición 60 - E/2016 de la DNPDP
- Recomendaciones de la UIT (Unión Internacional de Telecomunicaciones), organismo especializado de las Naciones Unidas (ONU) para las Tecnologías de la Información y la Comunicación – TIC.