Trabajo Final de Graduación

Ley 25.326 de Protección de Datos Personales. El derecho a la intimidad y el hábeas data como herramienta de protección y resguardo frente a Internet. Aplicabilidad en las provincias argentinas

Bernardi, Melisa Natalí

Abogacía

2016

Resumen

El presente Trabajo Final de Graduación, plantea como problema que, si bien el hábeas data es una herramienta de protección y resguardo de los datos personales en Internet, a la fecha, no todas las legislaciones provinciales se adecuan a la Ley 25.326 de Protección de Datos Personales y esto, determina el margen de aplicabilidad en cada una de ellas. La divulgación de datos privados, así como de estados de la vida personal parece no tener protección alguna cuando de informática se trata. La doctrina nacional acuerda –desde hace varias décadas- que, el derecho a la privacidad está íntimamente ligado a la libertad informática. De allí, necesidad de una regulación legal que garantice el derecho de verificar la exactitud, corrección, actualización o reserva de la información. En este marco surge, con la reforma de 1994, la incorporación del Artículo 43 con la figura del hábeas data, dentro del marco de acciones de amparo. Las numerosas las demandas sobre la aplicación del hábeas data frente a los avances tecnológicos y el almacenamiento de datos, hizo que en el año 2000 se dicte la Ley Nº 25.326 de Protección de Datos de Carácter Personal, la que reglamenta la acción del instituto citado. La misma, contiene –entre otros- los principios generales relativos a la protección de datos, los derechos de los titulares de datos, las obligaciones de responsables y usuarios de datos, el órgano de control, las sanciones y el procedimiento del recurso judicial hábeas data. Desde el Derecho Comparado se advierte que entre los países de Europa, existe un crecimiento relativo con respecto a la legislación. En los Estados americanos se manifiesta -como carácter común- la incorporación como cláusula constitucional en forma de hábeas data -o como acción de amparo-. Al analizar concretamente lo referido a las provincias argentinas en su conjunto, la realidad es disímil. Y, frente a esta realidad, la vulnerabilidad de las personas y su derecho personalísimo a la intimidad cuando del almacenamiento de datos informáticos se trata, exige la existencia de un marco regulatorio vigente en cada provincia argentina.

Palabras clave: derecho a la intimidad, libertad informática, derecho a la privacidad informática, hábeas data y Constitución, Ley 25.326 de Protección de Datos Personales, legislaciones provinciales.

Abstract

The present Final Paper of Graduation, poses as a problem that, although the habeas data is a tool of protection and protection of the personal data in Internet, to date, not all the provincial legislations are adapted to the Law 25.326 of Protection of Data Personal and this, determines the margin of applicability in each one of them. The disclosure of private data, as well as states of personal life seems to have no protection when it comes to computer science. National doctrine agrees - for several decades - that the right to privacy is closely linked to computer freedom. Hence, there is a need for legal regulation that guarantees the right to verify the accuracy, correction, updating or reservation of the information. In this context, with the 1994 reform, the incorporation of Article 43 with the figure of habeas data, within the framework of actions of amparo. The numerous demands on the application of habeas data in the face of technological advances and data storage, led in 2000 to issue Law No. 25,326 on Protection of Personal Data, which regulates the action of the institute cited. It contains - among others - the general principles relating to data protection, the rights of data subjects, the obligations of data controllers and users, the supervisory body, penalties and the procedure for judicial review . From the Comparative Law it is noticed that among the countries of Europe, there is a relative growth with respect to the legislation. In the American states, as a common character, the incorporation as a constitutional clause in the form of habeas data or as an amparo action is manifested. When analyzing concretely what refers to the Argentine provinces as a whole, the reality is dissimilar. And, faced with this reality, the vulnerability of people and their very personal right to privacy when it comes to storing computer data, requires the existence of a regulatory framework in force in each province of Argentina.

Key words: right to privacy, computer freedom, right to computer privacy, habeas data and Constitution, Law 25.326 on Personal Data Protection, provincial legislation

.

Índice

Introducción

El derecho a la intimidad, considerado como derecho personalísimo, se encuentra frente a un escenario complejo y abierto cuando se trata de avances tecnológicos referidos a la informática. En efecto, la intimidad constituye la faz privada de las personas y aquel lugar en el cual no le está permitido inmiscuirse a ninguna persona ajena a ella, tanto física como jurídica, ni pública como privada. Internet, parece manifestarse como enemiga de la protección de la privacidad al permitir el almacenamiento y circulación de datos personales por el cyberespacio, quitando todo manto de hermetismo y reserva que reposaba sobre cada individuo. Observada por algunos como la gran herramienta del mundo globalizado; para otros puede llegar a convertirse en un instrumento perverso y provocativo.

En este marco de avances tecnológicos y con la llegada de Internet se dibuja un nuevo escenario que marca claros desafíos para el mundo del Derecho. En este sentido, al llevarse a cabo la reforma constitucional de 1994, el Artículo 43 -tercer párrafo- introdujo la acción de amparo como la más idónea frente a la vulneración del derecho a la intimidad. Si bien, no menciona en forma expresa el concepto de hábeas data, entendido como el conjunto de informaciones que forman parte de la vida de una persona y que han sido expuestas en una base o banco de datos, queda reconocido a nivel constitucional el derecho a la protección de esos datos almacenados.

La doctrina nacional coincide en la vulnerabilidad de la persona frente al mal uso de los datos que se almacenan en la Internet y promueve un nuevo desafío para el mundo del Derecho; esto es, legislar en consecuencia, para que la intimidad de las personas no se vea avasallada ante la invasión de la informática.

De allí que la Ley 25.326 de Hábeas Data viene a cubrir aquella necesidad, otorgándole a cada persona el derecho de verificar la exactitud de estos datos, corregirlos, actualizarlos, exigir la reserva en cuanto a la circulación de los mismos, asegurando el amparo de la honra, los valores y el patrimonio de la vida privada de cada

ciudadano. Sin embargo y, a pesar de su entrada en vigencia en 2000, a la fecha encuentra una aplicación dispar en las distintas provincias argentinas.

Por esto, la presente investigación plantea como problema que: si bien el hábeas data es una herramienta de protección y resguardo de los datos personales en Internet, a la fecha, no todas las legislaciones provinciales se adecuan a la Ley 25.326 de Protección de Datos Personales y esto, determina el margen de aplicabilidad en cada una de ellas.

De acuerdo al problema planteado, el objetivo general busca analizar el margen de aplicabilidad de la Ley 25.326 de Protección de Datos Personales y su adecuación en el marco de las constituciones provinciales. Este objetivo se operacionaliza en los siguientes objetivos específicos: describir los alcances del derecho a la intimidad y a la privacidad informática desde la Constitución Nacional y las convenciones y pactos internacionales; profundizar en el análisis del articulado de la Ley 25.326 de Protección de Datos Personales; presentar fallos significativos de la jurisprudencia nacional referidos a la temática; identificar en la Comunidad Europea, América y las provincias argentinas los aportes del Derecho Comparado.

Por lo expuesto, el presente Trabajo Final de Graduación se organiza como sigue. En el Capítulo 1, se presentan los conceptos clave de derecho a la intimidad, libertad informática, derecho a la privacidad informática y derecho a la protección de datos, en el marco de la Constitución Nacional y los convenios y pactos de rango constitucional. En el Capítulo 2, se inicia el análisis de la Ley 25.326 de Protección de Datos Personales en sus primeros artículos, para continuar con el mismo en el Capítulo 3, agregándose además, tres fallos jurisprudenciales argentinos. En el Capítulo 4, se avanza sobre los aportes del Derecho Comparado desde la Comunidad Europea, América, para cerrar con las provincias argentinas. Por último, se arriba a las Conclusiones.

La irrupción de Internet en el mundo globalizado, desdibujó los límites del derecho a la intimidad reducido al ámbito de lo doméstico. La cantidad de datos que se

acumulan en la era de la informática parecen no tener control ni capacidad de cierre. Frente a esto, la legislación nacional ha avanzado desde la Constitución Nacional hacia una ley específica que promueva un marco protectivo al derecho a la intimidad, transformando el hábeas data en el mecanismo más idóneo. Sin embargo, la realidad en las provincias argentinas es disímil. Por esto, la difusión para el conocimiento del ciudadano común acerca de esta red de resguardo frente a la posibilidad de la violación del derecho a la intimidad; así como la concientización sobre la existencia de un marco regulatorio vigente en cada provincia argentina, justifica por sí solo la elección de esta temática de investigación.

Capítulo 1: Derecho a la intimidad. Libertad informática. El derecho a la privacidad informática. El derecho a la protección de datos

1.1. El derecho a la intimidad

El derecho a la intimidad de una persona o su fuero interno, aparece como prescrito cuando hace referencia al límite en el cual nadie puede inmiscuirse. En este sentido, puede definirse a la intimidad como aquellas cuestiones que hacen a lo vivido por la persona en su fuero íntimo y que no tiene porqué ser conocido por terceros ajenos al mismo. Aquí se incluye su intimidad familiar, su ideología política, sus pensamientos religiosos, entre otros. De acuerdo a Pizarro, *"(…) se trata de un derecho personalísimo integrado por tres aspectos fundamentales: tranquilidad, autonomía y control de información personal."* (Pizarro, 1991, 174)

El titular de este derecho cuenta con la facultad de oponerse a que su vida se vea afectada por distintas publicaciones que pueden aparece en la Internet o en las redes sociales, que implican la divulgación –no sólo de un conjunto de datos que, por su característica de privados, no deberían tomar estado público- sino y a la vez, estados de su vida personal.

Entonces, aquí se trata de no menoscabar la intimidad, de preservar el fuero íntimo exigiendo el respeto de la vida privada de cada persona, garantizándose el normal desenvolvimiento de su proyecto de vida, por lo que no se admiten -fuera de los casos permitidos por la ley-, intromisiones extrañas. (Santos Briz, 1963) Porque, en este marco se entiende el derecho a la intimidad vinculado a la publicidad de la vida privada en contextos virtuales en dos modalidades diferentes; esto es, aquellos espacios donde se requiere la carga de datos para el uso de tarjetas de crédito para pagos virtuales y, las redes sociales, donde la información puede viralizarse en pocos segundos. Estos dos temas serán tratados en el Capítulo 2 de este Trabajo Final de Graduación.

Continuando con el análisis, según Santos Cifuentes (García San Martín, 1995, Pág. 120) el derecho a la intimidad es el *"derecho personalísimo que permite sustraer a*

la persona de la publicidad o de otras turbaciones a la vida privada, el cual está limitado por las necesidades sociales y los intereses públicos." En otras palabras, este derecho personalísimo habilita, a un sujeto determinado, a controlar el uso que otros hagan de la información que le concierne, dado que es una necesidad humana vivir en un marco de dignidad, igualdad, y libertad que permita un desarrollo integral de la personalidad.

Entonces, el respeto a la vida privada y a la intimidad tanto personal como familiar se constituye en un valor fundamental del ser humano. Por esta razón, el mundo del derecho entiende la importancia de tutelarlo y dictar medidas para evitar que sea vulnerado, tanto como para subsanar los daños una vez ocasionados.

La vida privada y la intimidad son derechos complejos que se vinculan con otros, que pertenecen a la esfera íntima y personalísima de los sujetos; a saber: el derecho a la inviolabilidad del domicilio, de correspondencia y de las comunicaciones privadas; el derecho a la propia imagen, al honor, a no participar en la vida colectiva y a aislarse voluntariamente, a no ser molestado. Y, por último, el derecho a la privacidad informática, objeto de estudio de este informe y que será tratado más adelante en este Trabajo Final de Graduación.

Para finalizar este apartado, puede agregarse que la violación a la intimidad desde los medios informáticos, según Fronsini (1990, Pág. 40) *"(...) se verifica por medio de la elaboración cruzada de los datos que permiten la revelación de aspectos ocultos de la personalidad (...)"*. En otras palabras, la complejidad a la que remite la protección del sujeto frente a esta invasión a la intimidad está dada por la ausencia de agresión directa, sino más bien, por el transcurrir –casi silencioso- de la vida de una persona por los sistemas informáticos.

1.2. Libertad informática y el hábeas data en la Constitución

Frente al derecho a la intimidad, la libertad informática se impone como otro concepto de análisis. El concepto de libertad informática, según Puccinelli (1999) puede ser definido como

> *(…) aquella proyección del principio -valor- "libertad" que, aplicado a la actividad informática, se traduce en el derecho de los operadores de estos sistemas de colectar, procesar y transmitir toda la información cuyo conocimiento, registro o difusión no esté legalmente restringido por motivos razonables, fundados en la protección de los derechos de las personas o en algún interés colectivo, relevante que justifique tal limitación.* (Puccinelli, 1999, Pág. 66)

En este sentido, puede decirse que la libertad informática, por si sola no es una facultad que se le atribuye a un sujeto para hacer uso o disponer de la información almacenada en medios electrónicos. Más bien se habla aquí de una libertad frente al poder informático, que implica no asumirlo como mero instrumento de un sistema globalizado, el cual –según Bergel (1999, Pág. 30)- amenazaría los derechos fundamentales de los ciudadanos, de ser considerada más allá de esta concepción.

Por su parte, Herrero Tejedor (1992) sostiene que, esta libertad más bien determina *"(…) la libertad de controlar el uso de los propios datos personales insertos en un programa de informática. Es el hábeas data, correspondiente al antiguo hábeas corpus del respeto debido a la integridad y a la libertad de la persona."* (Bergel, 1999, Pág. 33) Esto es así, dado que muchos son los casos en los que no se encuentra una tutela adecuada para su protección.

De acuerdo a lo expuesto en el apartado anterior, la doctrina nacional acuerda que, el derecho a la privacidad está íntimamente ligado a la libertad informática. En este sentido, y desde la década del 80 del siglo pasado, referentes del Derecho como Bidart Campos (1995) y Bustamante Alsina (1986) ya habían señalado la vulnerabilidad de la persona frente al mal uso de los datos que se almacenan en la Internet; proponiendo a la vez, *"(…) agudizar el ingenio para que el derecho constitucional a la intimidad no*

quede burlado ante los adelantos y las invasiones de la informática." (Bidart Campos, 1995, Pág. 107)

En la misma línea argumentativa, Bustamante Alsina (1986) ya señalaba que

> *(...) en vista de los desarrollos crecientes de los sistemas de procesamiento automático de datos se hace impostergable una regulación legal que garantice a las personas el derecho de verificar la exactitud de los datos, su corrección o actualización, así como también que asegure la reserva de la información, salvo que exista un interés legítimo y que preserve la utilización de ella conforme a los fines para los que fueron recogidos.* (Bustamante Alsina, 1986, Pág. 119)

Los conceptos vertidos por Bidart Campos (1995) y Bustamante Alsina (1986) serían luego reflejados en la Ley 25.326 de Hábeas Data, la que será analizada en el Capítulo 2 de este Trabajo Final de Graduación.

Avanzando con el análisis, al hacer referencia al concepto de hábeas data, éste remite a un conjunto de informaciones que forman parte de la vida de una persona y que han sido expuestas en una base o banco de datos. En este sentido, el hábeas data –según Puccinelli (1998, Pág. 105)-

> *(...) busca asegurar el acceso a informaciones para la tutela de la honra, de la tranquilidad, del patrimonio, de la vida privada, entre diversos valores, contra los atentados efectuados por organismos públicos o de carácter público, en la anotación de datos e informaciones acerca de las personas.*

La Constitución Argentina, luego de la reforma de 1994, incorpora en su Artículo 43 la figura del hábeas data, dentro del marco de acciones de amparo *"(...) toda persona puede interponer acción expedita y rápida de amparo (...)"* (Constitución Nacional, Artículo 43) La doctrina argentina sostiene casi por unanimidad que se trata de una acción procesal constitucional. Así pueden citarse a Sagüés (1996), Bidart Campos (1995), Quiroga Lavié (1995), entre otros.

El Artículo citado en el tercer párrafo refiere a que: *"(...) Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes (...)"* (Constitución Nacional, Artículo 43) Cabe destacar aquí que, si bien no se hace explícito el concepto de hábeas data, se infiere como el recurso legal más idóneo para la protección del derecho a la intimidad y la privacidad informática. El hábeas data protege aquella información que identifica al individuo y por lo tanto es nominativa.

Cierra el tercer párrafo haciendo referencia a las acciones que pueden llevarse a cabo frente a la información registrada; esto es: *"(...) y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos."* (Constitución Nacional, Artículo 43)

La pluralidad de los derechos que ampara el hábeas data permite avanzar sobre la protección de los derechos de los titulares a otros espacios, donde la información recolectada es cedida a terceros.

Christensen (1999, Pág. 308) ha postulado que el instituto del hábeas data es *"(...) el medio idóneo para que todos los contribuyentes y responsables tomen conocimiento de los datos concernientes a ellos, en la calidad de tales, y requerir las correcciones o peticiones pertinentes y subsanar errores administrativos."*

Como sostiene Salazar Cano (2006), se trata de una subcategoría del procedimiento contemplado en la Constitución para proteger los derechos constitucionales y, por tanto, eleva la protección de datos personales a la categoría de derecho fundamental.

El Art. 43 ha tenido en la jurisprudencia, un amplio desarrollo –como podrá verse en el Capítulo 3 de este Trabajo Final de Graduación- excediendo, de alguna manera, los límites establecidos por dicha norma. Los numerosos casos presentados, las demandas sobre la aplicación del hábeas data frente a los avances tecnológicos y el

almacenamiento de datos, hizo que en el año 2000 se dictara la Ley Nº 25.326 de Protección de Datos de Carácter Personal, la que reglamenta la acción del instituto citado. La misma se trata en el siguiente Capítulo de este Trabajo final de Graduación.

1.3.El derecho a la intimidad en las fuentes internacionales constitucionalizadas

Los tratados de derechos humanos constitucionalizados por el Artículo 75, inc. 22 de la Constitución Nacional, a partir de la reforma de 1994, otorgan un marco adecuado a las disposiciones del Art. 43 analizado. Al mismo tiempo, regulan los aspectos relacionados con la privacidad de la siguiente manera:

1.3.1. Declaración Americana de los Derechos y Deberes del Hombre

En el marco de la Declaración, se establece –de acuerdo a su Artículo V- que: *"Toda persona tiene derecho a la protección contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar."* (Declaración Americana de los Derechos y Deberes del Hombre, 1948) Ya se ha hecho referencia al derecho a la privacidad, en los apartados anteriores, sólo cabe agregar que –en el caso del almacenamiento de datos, lo que se vulnera es el derecho a la reputación y la vida privada cuando su circulación se torna abusiva por la falta de control en el registro electrónico.

El Artículo IX, sostiene que: *"Toda persona tiene derecho a la inviolabilidad de su domicilio."* (Declaración Americana de los Derechos y Deberes del Hombre, 1948)Y, en este sentido, el dato de la locación domiciliaria se torna dato sensible porque abarca –de alguna manera- el estado de privacidad y anonimato al resguardo de la residencia privada. En otras palabras, lo que la doctrina considera como el *"standard" de la norma protectora del derecho a la privacidad de la correspondencia."* (Sagüés, 2007, Pág. 34)

Por último y siguiendo a Sagüés (2007), el Artículo X menciona que: *Toda persona tiene derecho a la inviolabilidad y circulación de su correspondencia."* (Declaración Americana de los Derechos y Deberes del Hombre, 1948) Aquí se estaría

frente a una interpretación amplia dado que considera en forma exclusiva, la protección de la correspondencia dentro del marco de la privacidad de las personas. En el caso de los registros de datos en la Internet, aún se torna dificultoso evitar la inviolabilidad de los correos electrónicos o las cuentas en las redes sociales.

1.3.2. Declaración Universal de los Derechos Humanos

En esta norma internacional, se advierte la amplitud interpretativa para que pueda ser aceptad y aplicada por los diferentes sistemas jurídicos internos. La interpretación extensiva que permite el Artículo 12, así lo confirma: *"Nadie será objeto de injerencias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o su reputación. Toda persona tiene derecho a la protección de la Ley contra tales injerencias o ataques".* (Declaración Universal de los Derechos Humanos, 1948)

1.3.3. Pacto Internacional de Derechos Civiles y Políticos

Dicha norma internacional, establece en su Artículo 17º Inc. 1, que: *"(...) nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación (...)"* (Pacto Internacional de Derechos Civiles y Políticos, 1966) Agregando en su Inc. 2 que todas las personas tienen el derecho a ser protegidas frente a las injurias o ataques contra su privacidad.

Fiel al espíritu de la Declaración Universal de los Derechos Humanos (1948) la norma introduce el concepto de *"ataques ilegales"* contra la vida privada de las persona, exhortando al Estado a que se convierta en garante de la preservación y protección de la intimidad de sus ciudadanos.

1.3.4. Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica)

El Pacto de San José de Costa Rica establece en su Artículo 11º Inc. 2, que *"Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación."* Y agrega en el inciso siguiente que el derecho a la protección, por parte de la ley, contra la invasión a la vida privada. (Pacto de San José de Costa Rica, 1969) Ambas normativas internacionales, refrendan el texto del Pacto Internacional sobre Derechos Civiles y Políticos (1966).

Para finalizar este apartado, cabe agregar que si bien los tratados de derechos humanos con jerarquía constitucional citados, no contienen –expresamente- disposiciones sobre el hábeas data, la doctrina sostiene que *"(...) cuando en alguna disposición de los mismos se hace referencia a derechos que se identifican con los que el hábeas data protege, se les debe dispensar el recurso sencillo y rápido (...)"* (Bidart Campos, 1995) que mencionan todas ellas. En efecto, al rastrear el concepto de recurso dentro de las normas analizadas se advierte, lo breve y efectivo frente a los tribunales competentes:

- En la Declaración Universal de Derechos Humanos, en su Artículo 8*: "un recurso efectivo (...) que la ampare contra actos que violen sus derechos fundamentales reconocidos por la constitución o por la ley."* (Declaración Universal de los Derechos Humanos, 1948)

- En la Declaración Americana de los Derechos y Deberes del Hombre, en su Artículo XVIII*: "un procedimiento sencillo y breve (...)* (que) *lo ampare contra actos (...)* (que violen) *los derechos fundamentales consagrados constitucionalmente."* (Declaración Americana de los Derechos y Deberes del Hombre, 1948)

- En la Convención Americana sobre Derechos Humanos, en su Artículo 25*: "un recurso sencillo y rápido o a cualquier otro recurso efectivo... que la ampare contra actos que violen sus derechos fundamentales reconocidos por la Constitución, la ley o la presente Convención."* (Pacto de San José de Costa Rica, 1969)

1.4. El derecho a la privacidad informática y el derecho a la protección de datos

En el marco de este Trabajo Final de Graduación de lo que se trata es de hacer explícito el derecho a la privacidad informática dado que pervive la facultad de cualquier sujeto de controlar la información personal que de él figura, tanto en los registros, archivos y banco de datos que se acumulan en la Internet.

Ahora bien, el derecho protegido durante el desarrollo del siglo XX, apuntaba más a las cuestiones de la privacidad entendida como un derecho de la soledad y garantía del individuo a la protección de la persona y de su seguridad, en el marco de su vida privada y doméstica. (Moeykens, 2000) Cuando irrumpe la informática y se comienzan a acumular datos o información sensible sobre los sujetos, el panorama de protección de este derecho personalísimo cambia en forma radical.

La informática se constituye en un instrumento o herramienta virtual que reemplaza al soporte papel en el cual se registraban desde los datos personales hasta patrimoniales de cualquier sujeto. Al mismo tiempo, la informática posibilita -por su rapidez-, la transferencia casi instantánea; el almacenamiento masivo de datos en poco espacio; la permanencia a perpetuidad de los datos y, su localización, modificación o borrado sin dejar rastros. (Cifuentes, 1995, Pág. 166)

En este sentido, el derecho a la intimidad –y en particular el derecho a la privacidad informática-, ha perdido su carácter individual y doméstico para adquirir una nueva significación; esto es, el traspaso de lo privado a lo público, con una dimensión colectiva y en la esfera social. En otras palabras, la exposición de los datos que se registran en la Internet deja de ser privada porque pueden ser utilizados o 'comunicados' de manera descontrolada para aprovecharlos con fines diferentes a los que fueron publicados o compilados. (Parellada, 1990)

Ahora bien, qué se entiende por dato. De acuerdo al Diccionario de la Lengua Española, un dato es un *"antecedente necesario para llegar al conocimiento exacto de una cosa o para deducir las consecuencias legítimas de un hecho (...) representación*

de una información de manera adecuada para su tratamiento por un ordenador". (Diccionario de la Lengua Española, 2001)

Obsérvese cómo, ya se encuentra incluida en la definición, la adecuación de la información para su tratamiento en la Internet. Luego, y ante la realidad descrita, se establece el derecho a la protección de datos. Por esto, y siguiendo a Pérez Luño (1991)

> *(…) la protección de datos personales tendría por objeto prioritario asegurar el equilibrio de poderes sobre y la participación democrática en los procesos de la información y la comunicación a través de la disciplina de los sistemas de obtención, almacenamiento y transmisión de datos.* (Pérez Luño, 1991, Pág. 144)

En este sentido y, siguiendo al autor, se estaría protegiendo *"el conjunto de bienes o intereses que puedan ser afectados por la elaboración de informaciones referentes a personas identificadas o identificables"* (Pérez Luño, 1991, Pág. 144)

Cabe agregar aquí que, Puccinelli (1999), distingue entre el derecho de la protección de datos y el derecho a la protección de datos. Respecto de primero sostiene que es el

> *(…) conjunto de normas y principios que, destinados o no a tal fin, y con independencia de su fuente, son utilizados para la tutela de los diversos derechos de las personas –individuales o jurídicas- que pudieran verse afectados por el tratamiento de datos nominativos.* (Puccinelli, 1999, Pág. 65-66)

Aquí se hace referencia a la utilización de los datos destinados a la protección de los derechos de las persona, más que a la protección de los datos en sí mismos. De igual manera, en la segunda definición, el autor refiere a la

> *(…) facultad conferida a las personas para actuar per se y para exigir la actuación del Estado a fin de tutelar los derechos que pudieran verse afectados*

por virtud del acceso, registro o transmisión a terceros de los datos nominativos a ella referidos. (Puccinelli, 1999, Pág. 65-66)

Sólo cabe destacar que, el autor entiende a estos conceptos como *"meramente instrumentales, es decir medios para la tutela de otros bienes jurídicos"* (Puccinelli, 1999, Pág. 65-66)

Por todo lo expresado, el suministro de datos personales, ha dejado de ser un problema individual o de clase –si se quiere- implicando, en la actualidad, a todos los sujetos con independencia de su condición económico-social. Esta es una consecuencia directa de la proliferación de bancos de datos y la compilación informática de datos personales en red.

Ejemplos de esto pueden ser los números de CUIL (Código Único de Identificación Laboral) o CUIT (Código Único de Identificación Tributaria) a los que se accede desde páginas públicas donde no se necesita registro previo alguno. Asimismo, la fecha de nacimiento, teléfono fijo, historia laboral, impuestos pagos o impagos, pueden verificarse desde las páginas de ANSES (Administración Nacional de la Seguridad Social), AFIP (Administración Federal de Ingresos Públicos), PAGINAS AMARILLAS –página comercial de las guías de empresas comercios servicios y profesionales de Argentina,-, VERAZ –es un organismo que maneja una gran base de datos con información sobre el estado financiero de persona o sociedad en cuanto al cumplimiento o incumplimiento de contratos-, entre otras.

La acumulación de datos que 'viajan' sin control por el espacio virtual de la Internet exponen a cada individuo que –alguna vez accedió al medio- a que sus datos personales, financieros, comerciales y hasta culturales, tendencias psicológicas, prácticas deportivas, etc. puedan ser consultados, manipulados, falsificados a voluntad de quien opere con ellos. (Parellada, 1990)

Ante este panorama, el hábeas data –de rango constitucional ya tratado- aparece como el medio judicial más idóneo para el ejercicio pleno del derecho a la intimidad y

la protección del derecho a la privacidad informática. Por esto, a continuación se realiza un análisis en profundidad de Ley 25.326 Hábeas Data que refiere a la protección de datos personales.

Capítulo 2: Ley 25.326 Hábeas Data. Protección de Datos Personales

En el presente Capítulo se realiza el análisis de los primeros artículos de la Ley 25.326, tarea que se continúa en el siguiente para vincularla con la jurisprudencia.

Como ya se expresara, la reforma de 1994 que incluye el Artículo 43 en la Constitución Nacional, receptó las exigencias que la doctrina y la necesidad de incluir los derechos de tercera generación, demandaban los nuevos tiempos dominados por las nuevas tecnologías, entre otros avances sobre la privacidad de las persona.

La posibilidad de conocer, rectificar, actualizar, suprimir y solicitar la confidencialidad de los datos personales que consten en registros o bancos de datos públicos o privados destinados a proveer informes, estipulada por aquel Artículo, demostró –además- la necesidad de reglamentar el hábeas data.

Así, en 2000, se promulga la Ley 25. 326 de Protección de Datos Personales que regula el hábeas data en Argentina y que, a la vez, desarrolla y amplía lo consignado por el Artículo 43. La misma, contiene –entre otros- los principios generales relativos a la protección de datos, los derechos de los titulares de datos, las obligaciones de responsables y usuarios de datos, el órgano de control, las sanciones y el procedimiento del recurso judicial hábeas data. Al mismo tiempo, expone los requerimientos para una 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.

A continuación, se realiza el análisis de los artículos más significativos, para luego, continuar abordándolos en el Capítulo siguiente.

2.1. Disposiciones y principios generales

El inicio de la Ley que se está analizando, establece el marco regulatorio en el cual se aplica el Artículo 43, párrafo tercero de la Constitución Nacional –ya referido *supra*-. En este sentido, el objeto de la presente Ley no es otro que el de la protección integral de los datos personales que se encuentren en almacenados en diferentes soportes, siendo estos archivos o bancos de índole pública o privada. En última instancia, no se busca más que el resguardo y protección –por parte del Estado- del derecho a la intimidad y privacidad informática, ya tratado con anterioridad.[1]

Sin embargo, parte de la doctrina cuestiona que este Artículo se limita a garantizar el derecho al honor y a la intimidad de las personas, cuando el Artículo 43 de la Constitución Nacional es más amplio en lo protectivo. Al mismo tiempo, cuestionan la aplicabilidad sobre las personas de existencia ideal, que bien se sabe no gozan del derecho a la intimidad. (Ekmekdjian, 1995) Por último, reclaman la ausencia de conceptos –explícitos- tales como la utilización informática de los datos personales.

Más allá de estas críticas, la misma doctrina reconoce el haber determinado como regulación legal el acceso a la información o datos almacenados de las personas. En este sentido, y siguiendo a Gozaini (2003), el acceso a la información

> *(…) es el corazón del sistema, desde que concreta el derecho que tiene toda persona para conocer los datos que se hayan registrado de ella, sean obtenidos de manera legítima o solapada (por medios desleales, fraudulentos o en forma contraria a como la ley lo dispone), y obtener a través de este conocimiento una vía rápida y expedita para resolver inmediatamente qué es lo que quiere hacer en adelante (actualizar, corregir, suprimir o plantear la confidencialidad).* (Gozaini, 2003, Pág. 61)

[1] **ARTÍCULO 1º**— (Objeto).
La presente ley tiene por objeto la 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, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.
Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal. En ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas. (Ley 25.326 Hábeas Data. Protección de Datos Personales, 2000)

2.1.1. Datos, bancos y bases de datos comprendidos

En el marco de esta Ley quedan establecidos los diferentes tipos de datos, el tratamiento de los mismos, quiénes son los titulares de los datos y aquellos definidos como usuarios. Así, en el Artículo 2º[2], se define que los datos personales son toda la información que involucre apersona físicas o no. La referencia que incluye lo que se entiende por datos sensibles, ampara a todos aquellos aspectos que definen a la persona desde en su fuero íntimo, porque prevalecen las opiniones, convicciones, afiliaciones sobre materia política, religiosa, moral, sindical; así como lo referido a la salud o la vida sexual.

Según Quiroga Lavié y Elman (2006, Pág. 8), este Artículo sigue al modelo español incluyendo una serie de definiciones que se apartan de la tradición legislativa de no considerar la pertinencia de incluir en las leyes una *"suerte de diccionario dentro de la ley"*. En este sentido, las definiciones sobre conceptos que son objeto de la regulación por parte de la Ley, aportan claridad a los actos legislativos; es el caso del enunciado que refiere a los datos informatizados, que son aquellos que, revistiendo el carácter de datos personales, son sometidos al tratamiento o procesamiento electrónico o

[2] **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, almacena-miento, organización o acceso.
— Tratamiento de datos: Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relaciona-miento, 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. (Ley 25.326 Hábeas Data. Protección de Datos Personales, 2000)

automatizado. Atentos a lo señalado por la Constitución Nacional, la finalidad de los archivos de datos no puede ofender a la moral pública; de allí la necesidad de un registro que los torne lícitos –de acuerdo al Artículo 3[3].

En el Artículo 4[4] se realiza una pormenorizada descripción que tiene que ver con los datos personales recolectados, su calidad y tratamiento. En este sentido, varios son los incisos que refieren a la certeza, veracidad, adecuación y pertinencia de los mismos. Por esto, los datos no deben ser recolectados por medios desleales o engañosos. De la misma manera, la actualización, supresión, sustitución o destrucción de los datos inexactos debe hacerse de manera periódica para el pleno ejercicio de los derechos de acceso del titular de los mismos.

2.1.2. El consentimiento libre, expreso e informado

Esta figura –que aparece en el Artículo 5[5]- corresponde a lo que se reconoce como otorgar la aprobación para el tratamiento de datos personales. Entendidos estos últimos

[3] **ARTÍCULO 3°** — (Archivos de datos – Licitud). La formación de archivos de datos será lícita cuando se encuentren debidamente inscriptos, observando en su operación los principios que, establece la presente ley y las reglamentaciones que se dicten en su consecuencia. Los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública. (Ley 25.326 Hábeas Data. Protección de Datos Personales, 2000)

[4] **ARTÍCULO 4°** — (Calidad de los datos).

1. Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.
2. La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley.
3. Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.
4. Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario.
5. Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el artículo 16 de la presente ley.
6. Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.
7. Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados. (Ley 25.326 Hábeas Data. Protección de Datos Personales, 2000)

[5] **ARTÍCULO 5°** — (Consentimiento).

1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias. El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 6° de la presente ley.
2. No será necesario el consentimiento cuando:
    a) Los datos se obtengan de fuentes de acceso público irrestricto;

como: nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio. La conformidad tiene las características de ser libre, expresa –en este caso por escrito- e informada.

En este sentido, el Artículo 6[6] de la misma Ley hace mención a qué tipo de información debe darse al titular, al momento de recabar datos personales; a saber: la finalidad, el registro en archivo, las consecuencias de otorgar los mismos, así como la posibilidad de acceso, rectificación o supresión de los datos otorgados.

2.1.3. Categorías y cesión de datos

Retomando la incorporación en el marco de esta Ley de los datos sensibles, el Artículo 7[7] refiere a la obtención y tratamiento de los mismos. Particularmente deja

---

b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;
c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio;
d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento;
e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526. (Ley 25.326 Hábeas Data. Protección de Datos Personales, 2000)

[6] **ARTÍCULO 6°** — (Información).
Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara:
a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios;
b) La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable;
c) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente;
d) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos;
e) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos. (Ley 25.326 Hábeas Data. Protección de Datos Personales, 2000)

[7] **ARTÍCULO 7°** — (Categoría de datos).
1. Ninguna persona puede ser obligada a proporcionar datos sensibles.
2. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.
3. Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros.
4. Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas. (Ley 25.326 Hábeas Data. Protección de Datos Personales, 2000)

establecido que no existirá obligación para persona alguna, en cuanto a proporcionar este tipo de datos, los cuales sí podrán ser recolectados, por ejemplo, con fines estadísticos sin identificación de sus titulares.

De la misma manera, el Artículo en análisis prohíbe la formación de archivos o bancos de datos sensibles, haciendo la aclaración sobre los datos religiosos, políticos y sindicales que pueden constar en registros que pertenezcan a estas diferentes organizaciones y sus miembros. Asimismo, menciona acerca del tratamiento de los datos penales que, sólo pueden ser tratados por autoridades competentes.

Siguiendo a Vanossi (1999) se debe

> *(…) asegurar que el uso de los bancos de datos no produzca una discriminación de aquéllos a quienes la información se refiere, utilizando los datos sobre cuestiones raciales, religiosas, políticas o sexuales de forma tal de configurar un campo informativo de carácter sensible, tendiente a manipular o desfigurar la imagen de las personas.* (Vanossi, 1999, Pág. 12)

Por su parte, el Artículo 11[8], refiere al momento de la cesión de los datos personales que pueden ser objeto de diferentes tratamientos. En este caso, se vuelve al Artículo 5 –ya mencionado- que expresa acerca del consentimiento informado y aclara

[8] **ARTÍCULO 11.** — (Cesión).
1. 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 con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo.
2. El consentimiento para la cesión es revocable.
3. El consentimiento no es exigido cuando:
   a) Así lo disponga una ley;
   b) En los supuestos previstos en el artículo 5° inciso 2;
   c) Se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias;
   d) Se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados;
   e) Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables.
4. El cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente y éste 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. (Ley 25.326 Hábeas Data. Protección de Datos Personales, 2000)

que, el mismo, en cuanto al suministro de datos, es revocable. Esta norma refuerza el cumplimiento de la Ley, para el caso de transferencias internacionales de datos, utilizadas cotidianamente desde los recursos informáticos.

2.2. Derechos de los titulares de datos

2.2.1. De información

En lo que refiere al derecho de información, ya se mencionó que es la cuestión medular de esta Ley, en su Artículo 13 establece que,

> *Toda persona puede solicitar información al organismo de control, relativa a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables. El registro que se lleve al efecto será de consulta pública y gratuita.* (Ley 25.326 Hábeas Data. Protección de Datos Personales, 2000)

Siguiendo a Vanossi (1999),

> *(…) toda persona debe poder controlar la información que le concierna. Se trata no sólo de impedir que nos invadan, sino también que se apoderen de nuestra intimidad y que la guarden, usen y difundan lejos de nuestro control. Este derecho confiere la facultad de acceder a los bancos de datos y de investigar su contenido.* (Vanossi, 1999, Pág. 12)

Para lograr el derecho a controlar la información que concierne a cada persona, de acuerdo al autor, no sólo debe habilitarse un acceso rápido a los bancos de datos, sino que –a la vez- debe permitirse en cualquier momento del procesamiento de esos datos para evitar irregularidades o alteraciones en los mismos. *"La regla de oro en tal sentido es exigir el conocimiento y consentimiento de cada interesado para que sus datos personales formen parte de los bancos y respecto a cómo serán utilizados."* (Vanossi, 1999, Pág. 12)

2.2.2. De acceso y contenido

En la misma línea argumentativa que el derecho a la información, el derecho de acceso -a la misma- queda registrado en el Artículo 14[9] de la Ley.

De acuerdo a los aportes de Vanossi (1999),

> *(…) el punto central de la protección de este derecho se encuentra en la obligación de aquéllos que almacenan datos personales y los sistematizan de poner en conocimiento de los interesados todas las circunstancias que hacen al funcionamiento de los bancos de datos.* (Vanossi, 1999, Pág. 13)

En efecto, el Artículo establece que la información solicitada debe ser proporcionada dentro de los diez días corridos a la solicitud. Y agrega que este derecho se ejerce en forma gratuita y por intervalos, siendo éstos, no inferiores a los seis meses.

En cuanto al contenido de la información, el Artículo 15[10] expresa que la misma debe ser clara y amplia, en lenguaje accesible y, que puede suministrarse por diferentes medios o soportes.

---

[9] **ARTÍCULO 14.** — (Derecho de acceso).
1. El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes.
2. El responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente. Vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará expedita la acción de protección de los datos personales o de hábeas data prevista en esta ley.
3. El derecho de acceso a que se refiere este artículo sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto.
4. El ejercicio del derecho al cual se refiere este artículo en el caso de datos de personas fallecidas le corresponderá a sus sucesores universales. (Ley 25.326 Hábeas Data. Protección de Datos Personales, 2000)

[10] **ARTÍCULO 15.** — (Contenido de la información).
1. La información debe ser suministrada en forma clara, exenta de codificaciones y en su caso acompañada de una explicación, en lenguaje accesible al conocimiento medio de la población, de los términos que se utilicen.
2. La información debe ser amplia y versar sobre la totalidad del registro perteneciente al titular, aun cuando el requerimiento sólo comprenda un aspecto de los datos personales. En ningún caso el informe podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con el interesado.
3. La información, a opción del titular, podrá suministrarse por escrito, por medios electrónicos, telefónicos, de imagen, u otro idóneo a tal fin. (Ley 25.326 Hábeas Data. Protección de Datos Personales, 2000)

2.2.3. De la rectificación, actualización o supresión

Continuando con el análisis del articulado de la Ley de hábeas data, el Artículo 16[11] menciona dentro de los derechos de los titulares de datos aquellos que permiten rectificar, actualizar o suprimir la información presente en bancos de datos.

En efecto, el titular -frente al responsable o usuario del banco de datos- puede interpelarlo para que en el término de cinco días hábiles aquéllos sean modificados. Este principio -junto al del Artículo 14 ya citado- dejan ver que, en Argentina, para la aplicación del hábeas data, el sujeto debe agotar una instancia administrativa o una interpelación extrajudicial previa, a los fines de iniciar una acción de protección de datos personales, frente al responsable o usuario del banco de datos.

Sólo cabe agregar que, mientras se producen las modificatorias o supresiones, el responsable del banco de datos deberá bloquear el archivo, haciendo exclusiva referencia a la información que existe en las redes informáticas.

2.3. Usuarios y responsables de archivos y bancos de datos

---

[11] **ARTÍCULO 16.** — (Derecho de rectificación, actualización o supresión).
1. Toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos.
2. El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad.
3. El incumplimiento de esta obligación dentro del término acordado en el inciso precedente, habilitará al interesado a promover sin más la acción de protección de los datos personales o de corpus data prevista en la presente ley.
4. En el supuesto de cesión, o transferencia de datos, el responsable o usuario del banco de datos debe notificar la rectificación o supresión al cesionario dentro del quinto día hábil de efectuado el tratamiento del dato.
5. La supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos.
6. Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable o usuario del banco de datos deberá o bien bloquear el archivo, o consignar al proveer información relativa al mismo la circunstancia de que se encuentra sometida a revisión.
7. Los datos personales deben ser conservados durante los plazos previstos en las disposiciones aplicables o en su caso, en las contractuales entre el responsable o usuario del banco de datos y el titular de los datos. (Ley 25.326 Hábeas Data. Protección de Datos Personales, 2000)

2.3.1. Registro de archivos y bancos de datos

Respecto del registro de archivos de datos, ya se ha expresado la necesidad de una inscripción para que sea lícito. Ahora bien, en el Artículo 21, se mencionan –entre otros- la información que debe suministrarse para dicho registro, el que será habilitado por el organismo de control.

Así reza el Artículo 21:

> *El registro de archivos de datos debe comprender como mínimo la siguiente información:*
> *a) Nombre y domicilio del responsable;*
> *b) Características y finalidad del archivo;*
> *c) Naturaleza de los datos personales contenidos en cada archivo;*
> *d) Forma de recolección y actualización de datos;*
> *e) Destino de los datos y personas físicas o de existencia ideal a las que pueden ser transmitidos;*
> *f) Modo de interrelacionar la información registrada;*
> *g) Medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información;*
> *h) Tiempo de conservación de los datos;*
> *i) Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos.*

Al mismo tiempo, no podrán poseerse datos personales distintos a los declarados en el registro, dado que el incumplimiento de cualquiera de estos requisitos, puede dar lugar a las sanciones administrativas previstas por la Ley.

Dichas sanciones del tipo administrativas están contempladas en el Artículo 31[12] de la Ley, a cargo del organismo de control y que van desde el apercibimiento, la suspensión a la multa.

En particular, en lo que refiere a la conformación de archivos o bancos de datos privados, la Ley en clara cuando expresa en su Artículo 24 que: *"Los particulares que formen archivos, registros o bancos de datos que no sean para un uso exclusivamente personal deberán registrarse conforme lo previsto en el artículo 21".* (Ley 25.326 Hábeas Data. Protección de Datos Personales, 2000)

2.3.2. Contrato de servicios informatizados de datos personales

La contratación de servicios informatizados de terceros, está incluida en la Ley, en el Artículo 25[13]. El mismo establece que los datos recabados y almacenados no podrán ser utilizados con otros fines que no sean los suscriptos en el contrato inicial. Y, que una vez cumplida la prestación contractual, los mismos deben ser destruidos.

En cuanto a la prestación de servicios de información crediticia, el Artículo 26[14], expresa que los datos recabados sólo deben ser de carácter patrimonial obtenidos en

[12] **ARTICULO 31.** — (Sanciones administrativas).
1. Sin perjuicio de las responsabilidades administrativas que correspondan en los casos de responsables o usuarios de bancos de datos públicos; de la responsabilidad por daños y perjuicios derivados de la inobservancia de la presente ley, y de las sanciones penales que correspondan, el organismo de control podrá aplicar las sanciones de apercibimiento, suspensión, multa de mil pesos ($ 1.000.-) a cien mil pesos ($ 100.000.-), clausura o cancelación del archivo, registro o banco de datos.
2. La reglamentación determinará las condiciones y procedimientos para la aplicación de las sanciones previstas, las que deberán graduarse en relación a la gravedad y extensión de la violación y de los perjuicios derivados de la infracción, garantizando el principio del debido proceso. (Ley 25.326 Hábeas Data. Protección de Datos Personales, 2000)

[13] **ARTÍCULO 25.** — (Prestación de servicios informatizados de datos personales).
1. Cuando por cuenta de terceros se presten servicios de tratamiento de datos personales, éstos no podrán aplicarse o utilizarse con un fin distinto al que figure en el contrato de servicios, ni cederlos a otras personas, ni aun para su conservación.
2. Una vez cumplida la prestación contractual los datos personales tratados deberán ser destruidos, salvo que medie autorización expresa de aquel por cuenta de quien se prestan tales servicios cuando razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se podrá almacenar con las debidas condiciones de seguridad por un período de hasta dos años. (Ley 25.326 Hábeas Data. Protección de Datos Personales, 2000)

[14] **ARTÍCULO 26.** — (Prestación de servicios de información crediticia).
1. En la prestación de servicios de información crediticia sólo pueden tratarse datos personales de carácter patrimonial relativos a la solvencia económica y al crédito, obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el interesado o con su consentimiento.

fuentes de acceso público, así como aquellos que demuestren el cumplimiento o no de las obligaciones de tipo patrimonial –de fuente de acreedores-; pudiéndose archivar o ceder datos que sean relevantes para confirmar o no la solvencia económica de los interesados.

2.4. Órgano de control: La Dirección Nacional de Protección de Datos Personales

La Dirección Nacional de Protección de Datos Personales constituido como el órgano de control, tendrá entre sus funciones las de asistencia y asesoramiento a quien lo requiera, el dictado de normas y reglamentaciones, la realización de los censos de datos, bancos y archivos de datos, imponer sanciones, constituirse en querellante, entre otras. Las referidas específicamente al control, refieren a: la observancia de las normas sobre integridad y seguridad de los datos de archivos y bancos; así como al cumplimiento de los requisitos y garantías que deben reunir los archivos o bancos de datos privados.[15]

---

2. Pueden tratarse igualmente datos personales relativos al cumplimiento o incumplimiento de obligaciones de contenido patrimonial, facilitados por el acreedor o por quien actúe por su cuenta o interés.
3. A solicitud del titular de los datos, el responsable o usuario del banco de datos, le comunicará las informaciones, evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y domicilio del cesionario en el supuesto de tratarse de datos obtenidos por cesión.
4. Sólo se podrán archivar, registrar o ceder los datos personales que sean significativos para evaluar la solvencia económico-financiera de los afectados durante los últimos cinco años. Dicho plazo se reducirá a dos años cuando el deudor cancele o de otro modo extinga la obligación, debiéndose hace constar dicho hecho.
5. La prestación de servicios de información crediticia no requerirá el previo consentimiento del titular de los datos a los efectos de su cesión, ni la ulterior comunicación de ésta, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios. (Ley 25.326 Hábeas Data. Protección de Datos Personales, 2000)

[15] **ARTÍCULO 29.** — (Órgano de Control).
1. El órgano de control deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley. A tales efectos tendrá las siguientes funciones y atribuciones:
a) Asistir y asesorar a las personas que lo requieran acerca de los alcances de la presente y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza;
b) Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por esta ley;
c) Realizar un censo de archivos, registros o bancos de datos alcanzados por la ley y mantener el registro permanente de los mismos;
d) Controlar la observancia de las normas sobre integridad y seguridad de datos por parte de los archivos, registros o bancos de datos. A tal efecto podrá solicitar autorización judicial para acceder a locales, equipos, o programas de tratamiento de datos a fin de verificar infracciones al cumplimiento de la presente ley;
e) Solicitar información a las entidades públicas y privadas, las que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos personales

El Artículo 30 refiere a los códigos de conducta[16] destinados a ser generados en aquellos espacios donde se realice el tratamiento de datos personales, con el objetivo de asegurar y mejorar las condiciones de las operaciones que le son propias a los sistemas informáticos. Estos códigos se encuentran bajo la observación del Organismo de Control.

Por último, en lo concerniente a las sanciones penales –las administrativas fueron expuestas *supra*- el Artículo 32[17] incorpora dos artículos del Código Penal; esto

---

que se le requieran. En estos casos, la autoridad deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados;
f) Imponer las sanciones administrativas que en su caso correspondan por violación a las normas de la presente ley y de las reglamentaciones que se dicten en su consecuencia;
g) Constituirse en querellante en las acciones penales que se promovieran por violaciones a la presente ley;
h) Controlar el cumplimiento de los requisitos y garantías que deben reunir los archivos o bancos de datos privados destinados a suministrar informes, para obtener la correspondiente inscripción en el Registro creado por esta ley.
2. Observado por D. 995/2000; B. O.: 30/10/2000.
3. El Director tendrá dedicación exclusiva en su función, encontrándose alcanzado por las incompatibilidades fijadas por ley para los funcionarios públicos y podrá ser removido por el Poder Ejecutivo por mal desempeño de sus funciones.(Texto según D. 995/2000 de Observaciones; B. O.: 30/10/2000). (Ley 25.326 Hábeas Data. Protección de Datos Personales, 2000)

[16] **ARTÍCULO 30.** — (Códigos de conducta).
1. Las asociaciones o entidades representativas de responsables o usuarios de bancos de datos de titularidad privada podrán elaborar códigos de conducta de práctica profesional, que establezcan normas para el tratamiento de datos personales que tiendan a asegurar y mejorar las condiciones de operación de los sistemas de información en función de los principios establecidos en la presente ley.
2. Dichos códigos deberán ser inscriptos en el registro que al efecto lleve el organismo de control, quien podrá denegar la inscripción cuando considere que no se ajustan a las disposiciones legales y reglamentarias sobre la materia. (Ley 25.326 Hábeas Data. Protección de Datos Personales, 2000)

[17] **ARTICULO 32.** — (Sanciones penales).
1. Incorpórase como artículo 117 bis del Código Penal, el siguiente:
"1°. Será reprimido con la pena de prisión de un mes a dos años el que insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos personales.
2°. La pena será de seis meses a tres años, al que proporcionara a un tercero a sabiendas información falsa contenida en un archivo de datos personales.
3°. La escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona.
4°. Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble del tiempo que el de la condena".
2. Incorpórase como artículo 157 bis del Código Penal el siguiente:
"Será reprimido con la pena de prisión de un mes a dos años el que:
1°. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;
2°. Revelare a otro, información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley. Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años". (Ley 25.326 Hábeas Data. Protección de Datos Personales, 2000)

es, el 117 y 157bis, donde se establecen las penas para aquellos que promuevan la inserción de datos falsos y/o viole la confidencialidad de los bancos de datos

Para cerrar este Capítulo, puede decirse que el avance que significa la aprobación y puesta en marcha de la Ley analizada, implica un enorme desafío para el Estado –en cuanto a su cumplimiento y control- y para cada uno de los usuarios de las redes informáticas, dado que el hábeas data sólo es un instrumento rápido y sencillo, cuando –quien demanda sobre el derecho a la privacidad vulnerada- está en conocimiento de los alcances de este instituto.

En el Capítulo siguiente, se avanza sobre los últimos artículos de la Ley y se los vincula con casos jurisprudenciales significativos.

Capítulo 3: Acción de protección de los datos personales y la jurisprudencia

Como ya se viene realizando desde el Capítulo anterior, en el presente se continúa con el análisis de los últimos artículos de la Ley 25.326, específicamente los referidos al Capítulo VII de la acción de protección de los datos personales.

3.1. Acción de protección de los datos personales

Con respecto a la acción de protección de los datos, es aquella que tiene como principal objetivo la protección al derecho de la intimidad con relación a los datos de una persona atento a ello la ley de protección de datos personales establece una clasificación de los datos que son objeto de protección por la referida acción. (Gil Domínguez, 1999)

3.1.1. Procedencia

La acción de protección de los datos personales procederá para la toma de conocimiento por parte del titular de dichos datos personales almacenados en un banco de datos para lograr su acceso, como así también, en el supuesto que corresponda en el caso de inexactitud, desactualización, etc. para lograr una rectificación, actualización o la supresión de un dato determinado, de acuerdo al Artículo 33[18] de la Ley analizada.

3.1.2. Legitimación activa y pasiva

Antes de iniciar el análisis de los artículos vinculados a esta temática, aparece como conveniente definir qué se entiende por legitimación activa y pasiva.

[18] **ARTÍCULO 33.** — (Procedencia).
1. La acción de protección de los datos personales o de hábeas data procederá:
a) para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos;
b) en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización. (Ley 25.326 Hábeas Data. Protección de Datos Personales, 2000)

Siguiendo a Ferreyra de De la Rúa (2003),

> *La legitimación sustancial activa supone identidad entre la persona a quien la ley le concede el derecho de acción y quien asume en el proceso el carácter de actor. Hay legitimación pasiva cuando existe identidad entre la persona habilitada para contradecir y quien ha sido demandado.* (Ferreyra de De la Rúa, 2003, Pág. 81)

En otras palabras, en la legitimación activa se hace referencia a quien interpone la demanda; mientras que, en la pasiva, se incluye al demandado. Tomando los aportes de Devis Echandía (1993), puede ampliarse la definición anterior respecto del demandante/demandado, al remitir a:

> *En lo que respecta al demandante, la legitimación en la causa es la titularidad del interés materia del litigio y que debe ser objeto de sentencia (procesos contenciosos), o del interés por declarar o satisfacer mediante el requisito de la sentencia (procesos voluntarios).* (Devis Echandía, 1993, Pág.10)

Y continúa diciendo:

> *Y por lo que al demandado se refiere, consiste en la titularidad del interés en litigio, por ser la persona llamada a contradecir la pretensión del demandante o frente a la cual permite la ley que se declare la relación jurídica material objeto de la demanda.* (Devis Echandía, 1993, Pág. 10)

Por último, cabe agregar los dichos de Chiovenda (1989), los que mencionan la relevancia de la identidad de la persona, más allá de la existencia del derecho:

> *Esta condición de la sentencia favorable se puede designar con el nombre de cualidad para obrar (...) preferimos nuestra vieja denominación de legitimatio ad causam (o legitimidad para obrar). Con ella se expresa que para que el juez estime la demanda, no basta que considere existente el derecho, sino que es*

necesario que considere la identidad de la persona del actor con la persona en cuyo favor está la ley (legitimación activa), y la identidad de la persona del demandado con la persona contra quien se dirige la voluntad de la ley (legitimación pasiva). (Chiovenda, 1989, Pág. s/d)

A los fines de analizar la legitimación activa se hace referencia concretamente a quién tiene el derecho para poder ejercitar la referida acción de protección de datos personales. Y así que, el Artículo 34[19] determina que, en primer lugar es el afectado quien puede ejercitar dicha acción, seguidamente de sus tutores, curadores, descendientes, como también aquellos que tengan un parentesco por línea colateral hasta el segundo grado.

Lo mencionado con anterioridad en el párrafo que precede, es con relación a las personas físicas. Pero además el mencionado Artículo acertadamente incorpora el supuesto de las personas jurídicas estableciendo que podrán ejercitar la acción sus representantes legales o apoderados.

La ley no refiere a si son personas jurídicas públicas o privadas, posiblemente se comprenda con un criterio, aquí, más extensivo. Por último, y de manera facultativa, admite la intervención del defensor del pueblo en el proceso, como coadyuvante, atendiendo a la locución *podrá* y no *deberá*.

En lo que respecta a la legitimación pasiva aquí hace referencia en relación a quién va dirigida la acción, por ende se materializan los responsables del manejo de los datos que son objeto de la demanda.

[19] **ARTÍCULO 34.** — (Legitimación activa).
La acción de protección de los datos personales o de hábeas data podrá ser ejercida por el afectado, sus tutores o curadores y los sucesores de las personas físicas, sean en línea directa o colateral hasta el segundo grado, por sí o por intermedio de apoderado.
Cuando la acción sea ejercida por personas de existencia ideal, deberá ser interpuesta por sus representantes legales, o apoderados que éstas designen al efecto. En el proceso podrá intervenir en forma coadyuvante el Defensor del Pueblo. (Ley 25.326 Hábeas Data. Protección de Datos Personales, 2000)

De esta manera es que el Artículo 35[20] –objeto de estudio de este informe- expresamente determina que se irá en contra de los responsables y usuarios tanto de bancos públicos, como privados, que se encuentran destinados a proveer informes.

3.1.3. Procedimientos

En lo referente al procedimiento aplicable; esto es, el trámite a seguir para su interposición ante el juez competente, debe dejarse en claro que el Artículo 37[21] -de la Ley en estudio-, hace una referencia a seguir como trámite principal. No obstante ello, determina una vía subsidiaria para el supuesto que, la vía correspondiente como principal no pueda ser articulada adecuadamente. Por lo tanto, el trámite predeterminadamente es el establecido en la Ley de hábeas data y supletoriamente se regirá por el Código Procesal Civil y Comercial de la Nación.

Lo anteriormente mencionado, hace referencia al trámite de juicio sumarísimo, ya que no se debe olvidar que la acción de hábeas data, como una de las especies del amparo, es una vía expedita y rápida y no se tramita por un procedimiento ordinario.

Hasta aquí, el análisis de la Ley 25.326. A continuación se presentan tres fallos vinculados a los aspectos mencionados en este Capítulo.

3.2. Los aportes de la jurisprudencia

En el presente apartado se realiza una breve descripción de tres fallos relevantes y de interés para dar cuenta de cómo, desde hace tiempo, se vienen vulnerando los datos personales, y cuál es la reacción legislativa al respecto.

---

[20] **ARTÍCULO 35.** — (Legitimación pasiva).
La acción procederá respecto de los responsables y usuarios de bancos de datos públicos, y de los privados destinados a proveer informes. (Ley 25.326 Hábeas Data. Protección de Datos Personales, 2000)

[21] **ARTÍCULO 37.** — (Procedimiento aplicable).
La acción de hábeas data tramitará según las disposiciones de la presente ley y por el procedimiento que corresponde a la acción de amparo común y supletoriamente por las normas del Código Procesal Civil y Comercial de la Nación, en lo atinente al juicio sumarísimo. (Ley 25.326 Hábeas Data. Protección de Datos Personales, 2000)

3.2.1. Unión De Usuarios Y Consumidores C/ Citibank S/ Sumarísimo. Buenos Aires, mayo 12 de 2006.

Para hacer una breve síntesis del siguiente caso jurisprudencial, puede mencionarse que como punto de principal resolución la Cámara debió tener en consideración si corresponde la interposición de un agravio colectivo en los términos de la Ley de Defensa del Consumidor –ya mencionada-; por un lado, analizando no sólo los aspectos constitucionales imperantes como los nuevos declaraciones y garantías sino a través de la Ley reglamentaria 25.326 analizada. Entonces, la principal cuestión a resolver está centrada en la legitimación activa para interponer esta determinada acción. Por parte de la Unión de Consumidores y Usuarios en contra de Citibank por utilizar datos de sus clientes para operaciones de marketing directo propio o de terceros, mediante el llenado de estas llamadas 'solicitudes de exclusión', sin el consentimiento respectivo.

El presente fallo jurisprudencial es una instancia de Cámara de Apelaciones en virtud de la cual se llega a la misma ante la presentación por la Unión de Usuarios y Consumidores de una acción de hábeas data colectivo en el que el juez *a quo* considera improcedente por carecer de legitimación en virtud de lo dispuesto por el Artículo 34 de la Ley 25.326 –abordado en el apartado anterior-, reglamentario del Artículo 43 de la Constitución Nacional.

Los agravios expresados en esta instancia -por la parte apelante- se fundamentan en que Citibank debe cesar en su operatoria para evitar que los datos personales de sus clientes sean difundidos como cedidos a terceras personas en violación al consentimiento expreso que exige la Ley al respecto.

Que ante esta situación, la parte apelada emitió una circular estableciendo la posibilidad de oposición que ante la no presentación de una documentación solicitando dicho cese se entiende la facultad expresa para poder utilizar esa información personal en forma discrecional.

Posteriormente, la accionada responde los agravios de la Unión de Usuarios y Consumidores aduciendo que debe rechazarse la medida solicitada atento a que no se procedió a la mediación previa obligatoria y que no existen intereses difusos en juego ni derechos colectivos de la acción, sino derechos individuales perfectamente determinados y determinables. Por tanto, no cabría la posibilidad de un proceso colectivo.

Como puntos centrales a analizar frente a los agravios esgrimidos y la contestación de la accionada, debe recordarse que –como se viene sosteniendo en este informe- el hábeas data tiene su raíz constitucional, a lo que se suma la legislación analizada en el Capítulo 2 con finalidad reglamentaria del citado artículo. Por lo dicho, el tribunal analiza que la relevancia del caso se encuentra en considerar la amplitud de la legitimación del alcance de lo que se consideran derechos colectivos o difusos que son objeto de protección de estas figuras jurídicas. Por lo que la Ley debe interpretarse armónicamente con el Artículo 43 de la Constitución Nacional, y no en forma aislada.

Es entonces que se plasman tres regímenes normativos que deben conjugarse; esto es, la Ley de Defensa del Consumidor Nº 24.240, la Ley de Hábeas Data 25.326 y la Constitución Nacional respectivamente. Esto es así porque, la primera Ley mencionada hace referencia a la protección de los derechos de los consumidores y usuarios, que en mención al citado fallo se ven avasallados, dado que los mismos ven afectados sus derechos al no estipularse previamente la situación en la cual se ven inmiscuidos, y siendo la entidad bancaria en este caso quien en su carácter de "profesional" se encuentra en una evidente situación de desproporción para con los usuarios; a lo que se agrega por otra parte la Ley de Hábeas Data mencionada a lo largo de este capítulo, y la que es objeto de este informe, que en este caso se ve en la necesidad de emplearse para proteger los derechos de los clientes de la entidad mencionada ut supra, con motivo de verse vulnerados en la manipulación de sus datos personales, y por último, la Carta Magna que completa el análisis desde su Artículo 43.

Por lo expresado, la actitud de exigencia por parte del banco de llenar un determinado formulario para solicitar el cese como medida o regla principal no se

condice con el espíritu de ninguna de las leyes citadas, por lo que se amplía la legitimación activa.

Así, la Cámara concluye en revocar la sentencia apelada y hacer lugar a la demanda intentada, condenando a Citibank a cesar en su operatoria tendiente a supeditar la prohibición de utilizar los datos de sus clientes para operaciones de marketing directo propio o de terceros, mediante el llenado de estas llamadas 'Solicitud de Exclusión' imponiendo costas a la vencida.

3.2.2. M. H. F. C/ BBVA Banco Francés S. A. S/ Hábeas Data. Mar del Plata, 22 De Febrero de 2010

Haciendo una breve síntesis del caso, puede observarse que en un primer momento, la Cámara se adentra en la consideración de analizar qué tipo de competencia corresponde ante la excusación efectuada -en una primera instancia-, que fue objeto de la interposición del presente recurso por parte del señor Matera en contra de la entidad bancaria. Y como segundo punto se centró en el alcance del Artículo 36[22] inciso b, de la Ley de hábeas data -ya nombrada en reiteradas oportunidades a lo largo de este informe y en los párrafos que anteceden-, a los fines de resolver la cuestión litigiosa.

En una primera instancia, se produce una excusación judicial remitiendo la causa al Juzgado Federal de Primera Instancia del Departamento Judicial de Mar del Plata que en turno corresponda, en virtud de la calidad de los datos que se encontraban por redes interjurisdicciones tanto nacionales como internacionales.

Como agravios expresados -en esta instancia por parte del doctor Federico Manuel Álvarez Larrondo- denota que no se trata de la procedencia de una competencia federal ya que se demanda a la entidad bancaria únicamente, para que la misma corrija

[22] **ARTÍCULO 36.** — Será competente para entender en esta acción el juez del domicilio del actor; el del domicilio del demandado; el del lugar en el que el hecho o acto se exteriorice o pudiera tener efecto, a elección del actor. Procederá la competencia federal: (…) Inciso b: cuando los archivos de datos se encuentren interconectados en redes interjurisdicciones, nacionales o internacionales.

los datos que se encuentran en su base, atento al procedimiento reglado –además-, por el Banco Central de la República Argentina.

Como se tiene conocimiento el Tribunal pasa a examinar el alcance del Artículo 36 de la Ley de Hábeas Data aduciendo que en un primer inciso exige que para que proceda la competencia federal debe encontrarse demandada una entidad oficial, cuestión que no se sucede en este supuesto fáctico, por lo que debe analizarse si se configura el otro requisito que es que, los datos se encuentren en redes interjurisdiccionales o interconectados.

Que la naturaleza de los datos manejados por parte del Banco Central son de naturaleza incorporadas en el Artículo citado, por lo que se manejan a través de redes informáticas como así también mediante Internet, por lo que se permite concluir que la manera de manejo de los datos pertinentes son de la misma naturaleza, aplicándose las disposiciones del Artículo en referencia.

De lo mencionado, la respectiva Cámara resolvió confirmar la sentencia apelada declarando procedente la excusación realizada -en primera instancia-, determinando de esta manera que la competencia correspondiente es la materia federal.

3.2.3. V. S. H. Recurso de Hábeas Data. Expediente Nº 1495-2012. San Nicolás de los Arroyos, 27 de marzo de 2013.

En los presentes autos caratulados la parte apelante -en tal cuestión- es VHS quien se encuentra considerado como ahijado procesal del Ministerio Público que realizara la investigación en concreto a los fines de determinar si existió una violación moral a la parte apelante. Por otro lado, se encuentra el Ministerio de Fiscalía General quien es la administradora del banco de datos fotográficos de personas que ostentan antecedentes delictivos a tal efecto.

La cuestión a resolver por parte de esta excelentísima Cámara de Apelaciones es determinar el alcance de la protección de los datos personales correspondientes, ya que

la parte apelante se vio afectada por verse incorporada en un banco de datos fotográficos, por un delito menor y sin descripción informativa alguna -resultando por ello afectada-, sintiendo temor y viviendo una transgresión moral a sus quehaceres diarios por esa situación.

Para ingresar al análisis del presente caso jurisprudencial en los autos caratulados V. S. H. Recurso de Hábeas Data. Expediente Nº 1495-2012, debe analizarse en primer lugar, el interés de la parte que interpone el respectivo recurso, otorgando como fundamento del mismo que existe un perjuicio a su integridad moral y personal al estar incluido en el sistema de archivos fotográficos llevados por parte de las Oficinas Técnicas de Identificación Personal ubicadas en cada Departamento Judicial del Ministerio Público Fiscal, sistemas que se encuentra compuesto por fotografías de autores de hechos delictivos.

Ante ello se contesta en esta primera instancia que, dicho sistema de gestión de datos son utilizados para la realización de reconocimientos fotográficos sin expresión de información personal y que además esta base de datos no es de carácter pública. Por esto, la jueza de primera instancia declara improcedente el recurso interpuesto.

Ante esta resolución denegatoria se procede su elevación a la Cámara de Apelaciones respectiva que analiza nuevamente el fondo de la cuestión en consideración a la expresión de agravios por parte de la parte apelante; considerando que cuando corresponde la procedencia del recurso de hábeas data analizando las condiciones requeridas por la Ley a los fines de la finalidad establecida del mismo.

La expresión de agravios en esta instancia es realizada por el defensor oficial expresando que se viola la garantía concretada en el Artículo 19 de la Constitución Nacional como así también en diversos tratados internacionales.

Ante esto, la Cámara de Apelaciones y Garantías en lo Penal del Departamento Judicial Zárate-Campana, dicta sentencia revocando lo dispuesto por la jueza de grado, y haciendo lugar a la acción de hábeas data planteada por V. S. H., ordenando a la Sra.

Fiscal General que -en el plazo de veinticuatro (24) horas- proceda a retirar las fotografías correspondientes al actor, existentes en los archivos fotográficos con que cuenta el Ministerio Público a su cargo, de conformidad con lo normado en la Ley N° 25.326 y Artículos 19[23] y 43 de la Constitución Nacional.

De la resolución expuesta llega como recurso extraordinario ante la Corte Suprema de Justicia de Buenos Aires quien realiza un estudio más profundizado de la causa estableciendo una comparación en la legislación provincial de hábeas data de Buenos Aires con la Ley nacional –ya tratada anteriormente-; aduciendo la necesaria implementación del trámite previo para la interposición del referido recurso.

En la consideración de la relevancia del caso planteado puede establecerse que el fondo de la cuestión debatida en estas instancias procesales se encuentra centralizado en el concepto de dato sensible según la legislación, debiéndose realizar una interpretación amplia del cuerpo normativo citado ya que como garantía constitucional no debe ser restringida, por lo que existió una clara violación al Artículo 4 inciso 7, Artículo 7 inciso 4, Artículo 23 incisos 2 y 3 de la Ley N° 25326, tratados en el Capítulo 2 de este Trabajo Final de Graduación.

Por lo que finalmente se ordena la supresión de los archivos fotográficos del apelante, confirmando de esta manera la sentencia de Cámara.

Para finalizar este Capítulo, puede decirse que, de acuerdo a los fallos recorridos, la acción del mundo jurídico sobre la protección de los datos y la aplicación del hábeas data como recurso más idóneo se confirma en los tres fallos presentados. No obstante, las limitaciones ya presentadas de la Ley 25.326 –en el Capítulo 2- aquí puede advertirse su plena vigencia y aplicación en torno a los damnificados que ven vulnerados su derechos a la privacidad y a la intimidad frente a la libertad informática.

[23] **ARTÍCULO 19.** 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. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe. (Constitución Nacional)

En el próximo Capítulo se avanza sobre los aportes del Derecho Comparado a nivel internacional, regional y provincial.

Capítulo 4: Derecho Comparado, internacional y nacional

La problemática alusiva al ya mencionado derecho a la protección de los datos personales, ha sido tratada en numerosas legislaciones de todo el mundo. A continuación se presentan –en breve síntesis- los aportes realizados desde el Derecho Comparado, para dar cuenta de aquellas normas que protegen a los ciudadanos –sujetos de derechos- frente a los avances y violaciones del mundo de la informática, en cuanto al manejo inescrupuloso –a veces- de los datos personales.

4.1. Comunidad Europea

La presente cuestión fue ocupada por diferentes organizaciones internacionales tal es el caso de la Organización para la Cooperación y el Desarrollo Económico (OCDE) representando una concientización acerca del aspecto internacional sobre los principios que deberían respetar los gobiernos, las empresas, y la sociedad en su conjunto para la protección de la privacidad y de los datos evitando restricciones arbitrarias en el manejo de ellos.

Y es interesante cómo la protección de los datos personales -como así también su manejo prudente- tiene una relación directa con la forma de gobierno que sirve a los fines de poder realizar una mayor y mejor comparación al respecto y tal como lo aclara Oyarzabal (2007, Pág. 71):

> *(…) en las últimas décadas, la mayoría de los países con régimen democrático liberal ha adoptado legislación protectora de la privacidad que en mayor o menor medida sigue los parámetros internacionales, lo que ha provocado un interesante -si no óptimo- nivel de armonización del derecho de los datos informatizados*.

En efecto, los estados miembros del Consejo Europeo, suscribieron en la ciudad de Estrasburgo, el 28 de enero de 1981, un Convenio para la Protección de Personas (Comunidad de Madrid, 2014), siempre relacionado a la problemática del tratamiento de

los datos de carácter personal. Este convenio tiene como principal objetivo, regular el tratamiento de datos, para de esa manera, proteger y darle el respeto que se merece a los derechos y libertades fundamentales de las persona físicas con independencia de su nacionalidad o su residencia.

Surge como elemento de gran importancia en el derecho europeo, la Directiva 95/46/CE de fecha 25 de octubre de 1995, del Parlamento Europeo y del Consejo. (Eur-lex, 2014) La misma hace referencia a la protección de las personas físicas y lo relacionado a la manipulación de los datos personales de cada individuo, así como la circulación de éstos con total impunidad. Esta Directiva crea un Grupo de Trabajo cuya función es evaluar a los Estados y a través de decisiones, determinar si se adecuan o no al grupo de los Estados que garantizan un apropiado nivel de protección de datos personales que se transfieren a la Comunidad. (Eur-lex, 2014)

Posteriormente, se declara la Carta de Derechos Fundamentales de la Unión Europea del año 2000 (Diario oficial de las comunidades europeas, 2000), reconoce el derecho a la protección de los datos personales, y agrega que deben tratarse con fines leales y con el consentimiento de la persona a la cual pertenecen aquéllos. Además, hace referencia a que todo individuo tiene derecho a solicitar el acceso a los datos que le conciernan y, de ser necesario, exigir su inmediata rectificación.

El fin que consagra el ya mencionado hábeas data, es el derecho que tiene toda persona de controlar los datos de carácter personal que existen en bancos de datos tanto públicos como privados. Es una garantía y un procedimiento judicial para ejercer tal control, a la par de ser un medio para resguardar de manera expedita, rápida y eficaz, los derechos vulnerados de una persona antes los excesos informáticos, entre otros.

A continuación, se realiza un recorrido por los más relevantes instrumentos y cuerpos normativos de Europa, detallando y analizando -en el caso de que existan-, las diferencias entre esquemas legislativos.

4.1.1. Portugal

En 1976, por primera vez, se reconoce en este país que era necesario proteger a las personas frente a los riesgos informáticos, pero a pesar de ello recién en 1991, fue consagrado legislativamente. En abril de ese año se dicta la Ley 10 de Protección de Datos Personales para hacerle frente a los excesos de la informática, tomando como base la Constitución portuguesa. Haciendo referencia a la misma, Portugal consagra el derecho que tienen los ciudadanos de tomar conocimiento de los datos que de ellos circulan en los registros informáticos, de igual manera que pueden exigir de ser necesario para ellos, la actualización o supresión, de esos datos sensibles. (Castillo Jiménez, 1993-1994)

Por ello, establece que el uso de la informática y de Internet debe realizarse de manera transparente y siempre respetando, la reserva que cada individuo tiene de su vida, tanto privada como los derechos y libertades, a los cuales accede en su carácter de ciudadano y persona.

Por otro lado, pero siempre relacionado a la problemática que le concierne, se crea la Comisión Nacional de Protección de Datos Personales, como órgano de aplicación. De esta manera, dicho ente se encarga de acoger los principios rectores relacionados al tratamiento de los datos de carácter personal del Consejo de Europa. (Castillo Jiménez, 1993-1994)

4.1.2. España

Al respecto la Constitución Española de 1978, en su cuerpo normativo hace referencia al honor, a la intimidad personal y familiar y a la propia imagen, considerados como derechos personalísimos. Además establece que la Ley limitará el uso de la informática para garantizar los derechos antes mencionados.

No obstante el reconocimiento constitucional, en la actualidad España cuenta con la Ley Orgánica 15/99 de Protección de Datos de Carácter Personal. El objeto de esta normativa es garantizar -como se dijo anteriormente-, todo lo relacionado a la manipulación de los datos personales, en especial lo relacionado al honor y la intimidad,

tanto familiar como personal. (Ley Orgánica 15/99 de Protección de Datos de Carácter Personal, España) Cabe aclarar aquí que, la Ley 25.326 está inspirada en esta normativa.

4.1.3. Francia

Francia, dictó en 1978 la Ley 753. La misma consagra el derecho que tiene toda persona a la información y al respeto por la privacidad, con relación a la administración y los ciudadanos, dicha Ley propone una serie de medidas que tienden a optimizar la relación existente entre estos dos polos y –asimismo- a todo lo relacionado con lo fiscal y lo social. (Ley 753/78, Francia)

4.1.4. Reino Unido

Este país ha sido objeto de importantes reformas relacionadas a la problemática latente. Por un lado, la Ley de Protección de Datos del año 1988, fue modificada luego de una consulta realizada en 1999. Y a la par de ello, se ha modificado también en el año 2000 la Ley de Acceso a la Información. (Estudio especial sobre el derecho de acceso a la información, 2007)

Para finalizar con este aparatado, puede observarse un crecimiento relativo en los países de Europa –como ya se expresara- con respecto a la legislación, atento al incremento tecnológico y al reconocimiento de los derechos humanos de tercera generación y de cómo estos últimos se ven afectados por la informática por un lado, así como también por la tecnología actual.

Puede advertirse como todo parte del reconocimiento que cada país tiene en su texto constitucional acerca de los derechos en análisis, y para ello es condición previa el examen del tipo de norma fundamental que se adopte. Esto dependerá de que se esté frente a un texto constitucional de sistema abierto o cerrado para la incorporación del derecho a la intimidad y a la protección de los datos personales.

De acuerdo a lo expresado, cabe destacar que, entre los países de Europa que tienen un reconocimiento expreso en su texto constitucional de los derechos de la protección de los datos personales, a Portugal, por haber sido el primero en realizar este reconocimiento expreso en el año 1976. Luego, vendrían varios países europeos.

Otros países denotan que, si bien tienen regulación constitucional, el carácter de esta incorporación es de manera implícita o subyacente dentro de otros derechos reconocidos a lo largo del texto de su ley fundamental. Tal el caso de España, que en su sistema jurídico si tiene menciones al respecto y, regula -en la actualidad- a través de la Ley Orgánica 15/99, siendo seguido por otros países.

Por último, también se encuentran los Estados en donde no se hace referencia expresa en su legislación constitucional a lo referente a la protección de los datos personales. Aunque sin perjuicio a ello, sí se encuentran ubicados dentro de otros derechos fundamentales, reconocidos por la jurisprudencia, como así también por la doctrina.

Comparando con la República Argentina y en base a los países europeos analizados, puede decirse que, son distintas las maneras en las que se encuentra regulada esta institución del derecho atinente a la protección de los datos personales. Argentina tiene una constitución de sistema cerrada o llamada pétrea por lo que su modificación no es sencilla sino por convención constituyente, debe aclararse que toda la incorporación referida estuvo determinada por la reforma del año 1994 que posteriormente fuera materia de la sanción de la Ley de hábeas data. Con ello quiere establecerse, en carácter expreso, que Argentina tiene respeto por la protección de los datos personales, al igual que varios países de Europa. Más aún, la legislación ahonda en la temática a través de la ley de hábeas data de naturaleza tanto de fondo como de forma que regula el mismo de manera mucho más precisa.

4.2. América

4.2.1. Estados Unidos

Se sanciona en 1966, la Ley de Libertad de Información -FOIA en alusión a las sigla en inglés The Federal Freedom of information act-. Luego de una década se dicta una enmienda haciendo alusión a los documentos electrónicos. Recién en 1974, se sanciona la Ley de Privacidad, ya que el concepto de privacidad surge tanto en la doctrina como en la jurisprudencia a fines del siglo XIX, tal y como se ha visto en el Capítulo 1 de este informe.

Esta Ley dota al ciudadano de todo derecho a consultar la información que sobre su persona posee el Estado, y lo faculta a solicitar la corrección, así como también a poner en conocimiento de cuándo y con qué fines es usada su información por las entidades públicas. De igual manera, se crea para la vulneración maliciosa de esos datos, una acción civil ante los tribunales para demandar por daños y perjuicios. (Ley de Privacidad, 1974, EE.UU.)

4.2.2. Brasil

Fue el primer país de la región en contemplar el hábeas data en el año 1988 en su Constitución. En este cuerpo normativo se señala que la persona tiene la facultad de acceder mediante el hábeas data, al conocimiento de la información que de ella consten en registros o bancos de datos de entidades gubernamentales, o asimismo de carácter privado. Y hace referencia –además- a que la misma puede solicitar la rectificación de esos datos, cuando sean incorrectos o perjudiciales. Consagra la gratuidad de este procedimiento y señala que puede llevarse a cabo tanto por procedimiento judicial como administrativo. (Constitución, 1988, Brasil)

4.2.3. Paraguay

Su Constitución –a partir de 1992- consagra la figura del hábeas data, a toda persona que quiera acceder a la información y a los datos que de ella figuran, sean éstos personales o bienes propios, que figuren en registros oficiales o privados, para que el afectado pueda conocer el uso y la finalidad que se les da.

Es por eso que es de gran envergadura lo relacionado a la competencia y la responsabilidad que deben tener los magistrados. La misma Constitución señala que si éstos se negaran sin justificación suficiente, a entender en esta cuestión, serán enjuiciados y de ser factible removidos de su cargo. (Constitución, 1992, Paraguay)

4.2.4. Perú

La Constitución de Perú, establece la acción de hábeas data –a partir de 1993-, como una garantía para todas aquellas personas que vean afectado su derecho cuando deseen solicitar a alguna autoridad información acerca de los datos que de ella consten, y ésta se lo niegue. También hace referencia en el caso de que lo solicite sin causa alguna, siempre y cuando afecten la intimidad personal y los denominados datos sensibles. Asimismo, sanciona en el año 1994 la Ley N° 26.301, la que establece la competencia para la tramitación de la acción de hábeas data. (Constitución, 1993, Perú)

4.2.5. Chile

En coincidencia con Argentina, se dicta en el año 2000 la Ley de Protección de Datos de Carácter Personal Nº 19.628. La misma tiene por objeto proteger los datos personales, pero únicamente de personas físicas, y de igual manera pone una especial atención al contenido de los datos sensibles, pero no hace referencia alguna al tratamiento de los mismos. (Ley de Protección de Datos de Carácter Personal, Nº 19.628, Chile)

4.2.6. Uruguay

Primeramente Uruguay contó con la Ley 17.838 de 2004, para una regulación en lo referente a los datos de naturaleza comercial, como también respecto a los secretos de correspondencia y normativa legal que abarca también al secreto profesional.

Con posterioridad, en 2008, y ante la necesidad de una normativa más concreta en lo referente a la protección de los datos, se sancionó la Ley 18.331 que es la que rige

actualmente y deroga a la anterior, siendo de carácter más extensa, y específica que su antecesora. (Ley 18.331, Uruguay)

Como se advierte, posteriormente al análisis individual de algunos países del Continente Americano, puede verse que el norte presenta una realidad normativa diferente a la de América del Sur. En efecto, en EE.UU. ya desde 1980 existe una regulación atinente a este tema. En el resto del continente la regulación legal de los datos personales devino más tarde, donde el crecimiento informático fue paulatino como ya se ha mencionado.

Puede concluirse, entonces, que los Estados americanos manifiestan -como carácter en común- que la temática referente a los datos personales fue incorporada en una modalidad de cláusula constitucional en forma de hábeas data -o como acción de amparo-. Luego vendría la regulación -en leyes especiales- que codifican la materia.

Sin embargo, y a partir de lo dicho debe reconocerse que no son unánimes las disposiciones referentes a la protección de los derechos vinculados a los datos y su almacenamiento, esta falta de uniformidad no permite una protección homogénea y efectiva frente a un proceso de globalización inmerso de tecnologías de intercomunicación.

Como referencia en común, un dato no menos importante a lo suscripto anteriormente, se deduce de los países integrantes del MERCOSUR que se han comparado en este informe, tales como, Brasil, Perú, Chile, Paraguay y Uruguay, en ninguna de estas naciones se ha creado o establecido un organismo independiente del Poder Ejecutivo, lo que determinaría una necesidad imperante a los fines del ejercicio correcto y transparente del poder de soberanía sobre los administrados.

Para el caso de la República Argentina, el denominado hábeas data presenta de ser una modalidad variable o también podría considerarse como un subtipo del amparo general del Artículo 43 de la Constitución Nacional. Se presentó a través de una inserción de una norma especial y que tiene reconocimiento constitucional.

Y como lo establece Muñoz del Alba Medrano *"se trata de proteger a la persona frente a la indefensión por el mal uso y la publicación de sus datos*." (2004, Pág. 11) Los principios de protección de datos personales se encuentran presentes en la Constitución Nacional de la República Argentina, en la Ley de Hábeas Data y en las Constituciones Provinciales, que en algunos casos se originaron antes que la Ley Nacional. Hábeas Data, Protección de Datos, Argentina, Ley 25.326, Decreto 1558/2001 y Disposiciones al respecto. Con todo ello se quiere hacer referencia a que la República Argentina ha respetado los lineamientos normativos constitucionales relativos al tema aquí tratado por lo que no hay consideraciones adicionales.

Al llegar a este punto, se presenta la situación en las diferentes provincias argentinas, con el fin de dar respuesta al problema planteado para este Trabajo Final de Graduación; esto es que: si bien el hábeas data es una herramienta de protección y resguardo de los datos personales en Internet, a la fecha, no todas las legislaciones provinciales se adecuan a la Ley 25.326 de Protección de Datos Personales y esto, determina el margen de aplicabilidad en cada una de ellas.

4.3. Provincias argentinas

Haciendo referencia a la protección de los datos personales, puede decirse que en Argentina, antes de ser consagrado a nivel nacional todo lo relacionado a ello, fue tratado en el derecho de las provincias. A continuación, se presenta una breve reseña de las provincias que ofrecen tratamiento respectivo de este derecho.

4.3.1. Córdoba

La Constitución de la provincia de Córdoba -del año 1986- menciona el derecho a la privacidad en el Artículo 50, referido al derecho que tiene toda persona a conocer lo que de ella conste en forma de registro, así como también la finalidad a que se destinan los mismos, y a reclamar y exigir de ser necesario para ella la pronta rectificación y actualización.

De acuerdo al Artículo 50:

> *Toda persona tiene derecho a conocer lo que de él conste en forma de registro, la finalidad a que se destina esta información, y a exigir su rectificación y actualización. Dichos datos no pueden registrarse con propósitos discriminatorios de ninguna clase ni ser proporcionados a terceros, excepto cuando tenga un interés legitimo*. (Constitución de Córdoba, 1986)

Por otra parte, y siguiendo con la privacidad y el derecho de los ciudadanos, menciona que los datos sólo podrán proporcionarse a terceros interesados de manera excepcional cuando tengan un interés legítimo, pero agrega también que no podrán ser utilizados con propósitos discriminatorios. *"(...) La Ley reglamenta el uso de la informática para que no se vulneren el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos."* (Constitución de Córdoba, 1986)

Queda establecido que el uso de la informática, es reglamentado por ley, de manera tal que no afecte la intimidad personal ni familiar. Además todo lo hasta aquí expresado, la provincia de Córdoba cuenta con una ley novedosa y actual respecto al tema planteado; esto es, la Ley 9.380 de Regulación del uso de videocámaras en lugares públicos sancionada en abril del 2007. Ésta cuenta con quince artículos en los cuales designa en primer lugar, el ámbito de aplicación, establecido en su Artículo 1:

> *(...) en la vía publica, en lugares públicos o de acceso público, a través de cámaras y/o videocámaras y/o cualquier otro medio técnico análogo y/o cualquier otro sistema utilizados por fuerzas de seguridad públicas (...)* (Artículo 1, Ley 9.380 de Regulación del uso de videocámaras en lugares públicos, 2007)

Al mismo tiempo, establece la finalidad del uso de este sistema, el cual contribuye a *"(...) la instrucción, coordinación y colaboración en la investigación y prevención de contravenciones y delitos."* (Artículo 1, Ley 9.380 de Regulación del uso de videocámaras en lugares públicos, 2007)

De manera similar, en el Artículo 10 de la Ley 9.380, hace mención que en caso de incumplimiento a los deberes planteados, de confidencialidad, será considerado falta grave, correspondiendo a los infractores las sanciones previstas, ya sea en el estatuto correspondiente o en el régimen general que regula el procesamiento informático de datos de carácter personal vigente. Sin perjuicio de las sanciones penales que le correspondieren.

Como puede observarse, la reglamentación es clara en cuanto a la protección de los ciudadanos frente a los datos y/o imágenes captadas o registradas a través del procesamiento informático, convirtiéndose la provincia de Córdoba en pionera del tratamiento de esta temática en su Constitución.

4.3.2. Río Negro

No menos novedosa es la Constitución de la provincia de Río Negro, que ya en el año 1988, tras una nueva reforma, incluye la protección de la intimidad de las personas, frente a diferentes tratamientos informáticos que pueden realizarse con los datos que se acumulan.

En efecto, en el Artículo 20 de la Constitución provincial, se hace referencia al derecho a la privacidad estableciendo que la ley garantiza la intimidad de las personas. Y de manera similar hace referencia al uso de dicha información, diciendo que ésta debe ser almacenada, procesada o destruida mediante un medio físico electrónico. Y agrega que debe propender siempre a respetar el honor, la privacidad y el goce completo de los derechos.

Así, el Artículo 20, menciona que:

> *La ley asegura la intimidad de las personas. El uso de la información de toda índole o categoría, almacenada, procesada o distribuida a través de cualquier medio físico o electrónico, debe respetar el honor, la privacidad y el goce completo de los derechos.* (Constitución de Río Negro, 1988)

Por otra parte, el Artículo mencionado refiere a los principios de justificación social, para el uso de los datos recogidos, los que pueden ser limitados en su recolección. Y, asegura que toda persona que haya sido afectada por el uso de información no veraz, puede acceder a la misma para *"(...) su rectificación, actualización o cancelación cuando no fuera razonable su mantenimiento."* (Constitución de Río Negro, 1988)

Posteriormente en 1998, la provincia de Río Negro, sanciona la Ley Nº 3.246, de Acción de Hábeas Data, la que hace referencia en su cuerpo legal –en el Artículo 1- a que la acción corresponderá cuando a toda persona –física o jurídica-

> *(...) se le niegue el derecho a conocer gratuita e inmediatamente todo dato quede ella o sobre sus bienes conste en registros o bancos de datos públicos pertenecientes al Estado provincial y los municipios y en similares privados destinados a proveer información a terceros (...)* (Artículo 1, Ley 3.246 de Acción de Hábeas Data, 1998)

A la vez, agrega que *"(...) en caso de falsedad o discriminación (...)"* el damnificado podrá *"(...) exigir su supresión, rectificación, confidencialidad o actualización".* (Artículo 1, Ley 3.246 de Acción de Hábeas Data, 1998)

Por último agrega los procedimientos a llevar a cabo en caso de faltas a las obligaciones por ella impuestas.

Junto a la provincia de Córdoba –en cuanto a sus constituciones- Río Negro aporta la novedad de una ley exclusiva que contemple la acción de hábeas data en forma temprana.

4.3.3. Buenos Aires

Ya en la década del ‘90, en su respectiva Constitución -de 1994-, Buenos Aires incluye el hábeas data, otorgándole rango constitucional -de manera expresa-, aunque luego, será reglamentada por ley. En efecto, en su Artículo 20, Inciso 3, reza: *“(...) A través de la garantía de Hábeas Data que se regirá por el procedimiento que la ley determine (...)”* (Constitución de Buenos Aires, 1994)

El mencionado Artículo, establece que toda persona podrá conocer lo que de ella figure en forma de registro, banco o archivos de organismos públicos como privados, que sean destinados a suministrar informes. De igual manera, los ciudadanos están facultados a requerir información acerca de cuál es la finalidad a que se destina aquella y, a requerir su actualización, rectificación o cancelación.

Al igual que las constituciones analizadas hasta aquí, incluye la prohibición del uso de los datos almacenados con fines discriminatorios y con respecto a proporcionarlos a terceras personas, sólo puede hacerse cuando éstos tengan un interés legítimo y fundado. Además establece que el uso de la información no podrá quebrantar de ninguna manera el ejercicio pleno de los derechos, así como también en honor y la intimidad tanto personal como familiar. *“(...) Ningún dato podrá registrarse con fines discriminatorios ni será proporcionado a terceros, salvo que tengan un interés legítimo. El uso de la informática no podrá vulnerar el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos.”* (Constitución de Buenos Aires, 1994)

Además de lo ya expuesto, la provincia de Buenos Aires cuenta con la Ley 14.214 de Hábeas Data, sancionada en 2010, en su Artículo 5, -en concordancia con el Artículo 20 inciso 10, mencionado con anterioridad- establece el procedimiento a llevar a cabo en caso de infracción. A la vez establece quiénes son los legitimados activa y pasivamente, y la jurisdicción competente. “(…) *El peticionante deberá notificar fehacientemente su pretensión al titular del banco de datos o registro. Solo ante la negativa o silencio de éste quedará expedita la acción judicial (...)”* (Artículo 5, Ley 14.214 de Hábeas Data, 2010)

En coincidencia con las leyes ya analizadas, puede agregarse que, Buenos Aires sanciona la ley de hábeas data, en la primera década del presente siglo.

4.3.4. Chaco

La provincia de Chaco recepta en su cuerpo normativo principal, la figura de hábeas data, incorporada en ella en el año 1994, año en que fue realizada la reforma con el objetivo -entre otros- de incorporar el Artículo 19, el cual coincide en su extensión, con lo ya tratado en las constituciones anteriores.

> *(…) Todos los derechos y garantías reconocidos, expresa o implícitamente, en esta Constitución, están protegidos en sus ejercicios por las siguientes acciones: (…) Toda persona tiene derecho a informarse de los datos que sobre sí mismo, o sobre sus bienes, obren en forma de registro o sistemas oficiales o privados de carácter público; la finalidad a que se destine esa información, y a exigir su actualización, corrección, supresión o confidencialidad. Tales datos no podrán ser utilizados con fines discriminatorios de ninguna especie. (…)* (Constitución de Chaco, 1994)

El mismo hace referencia a que toda persona tiene el derecho de conocer lo que de ella figure en registros o sistemas oficiales, así como también a la supresión o corrección de esos datos en caso de errores.

Posteriormente, se sanciona -en el año 1996-, la Ley 4.360 de Hábeas data, que viene a regular todo lo atinente a la interposición de la acción en caso de malversaciones de datos de los ciudadanos. La misma en su cuerpo normativo, hace referencia a la interposición de la acción, procedencia, improcedencia, competencia, requisitos y forma de la demanda, la prueba y los recursos. En otras palabras, es un verdadero cuerpo normativo donde se explicitan las formas de llevar a cabo esta acción.

4.3.5. San Juan

La respectiva Constitución -de 1996- dice que todo ciudadano tiene el derecho a conocer lo que de él conste en los registros y la finalidad con que tales datos sean utilizados. Con la facultad de solicitar de ser necesario su inmediata rectificación y/o actualización.

La Constitución -en su Artículo 26- establece que la informática no podrá bajo ningún punto de vista utilizarse como dato acumulable, todo lo referido a la fe religiosa, convicciones políticas, vida privada, etc. Con una excepción, cuando esa información antes mencionada sea utilizada con fines estadísticos sin posibilidad de identificar a los participantes. (Constitución de San Juan, 1996) Obsérvese cómo, esta Constitución ya incluye lo referido a datos sensibles, que luego serán incluidos en el Artículo 2 de la Ley 25.326, tratada en el Capítulo 2 de este Trabajo Final de Graduación.

Además de ser mencionada en la Constitución sanjuanina, la figura de hábeas data aparece en la Ley 7.447 de Registros Públicos de Banco de Datos, sancionada en 2006, de manera explícita.

Están habilitados para ejercer la acción, *"todo ciudadano que se crea afectado en su derecho a causa de la registración de datos, producción de informes por parte de las empresas dedicadas a ello, podrá reclamar el cese de la situación por procedimientos expeditos o sumarísimos (...)."* (Artículo 10, Ley 7.447 de Registros Públicos de Banco de Datos, 2006)

Y, el mismo Artículo agrega que:

> *(...) Igual derecho asistirá a aquel que estando correctamente incorporado a las listas de morosos, no fuera inmediatamente excluido, sin necesidad de requerimiento previo, de tal inhabilitación o interdicción en el ejercicio parcial o total de actos de la vida civil, una vez extinguida su condición de deudor.* (Artículo 10, Ley 7.447 de Registros Públicos de Banco de Datos, 2006)

La Ley hace referencia a la personas físicas o jurídicas que como actividad se dediquen a almacenar datos o informes deberán estar inscritas en el Registro Público de Comercio, y agrega que los datos podrán incorporarse a los registros e informes, únicamente si son suministrados por el deudor, acreedor o toda persona autorizada para emitirlos.

A su vez, menciona los plazos de avisos para el dueño de los datos, en diez días anteriores al posible uso de los informes obtenidos y la finalidad que se le dará.

Sin perjuicio de lo mencionado, la persona dueña de los datos, podrá –dentro de esos diez días- requerir la corrección, o supresión de lo que no corresponda o que resulte erróneo. Sin más trámite, los responsables deberán en el plazo de 72 horas, responder al interesado lo resuelto acerca de lo peticionado. (Ley 7.447 de Registros Públicos de Banco de Datos, 2006)

4.3.6. Chubut

El hábeas data se encuentra tratado en la Constitución de la provincia reformada en 1994, en su Artículo 56, sin que aparezca explícitamente, más bien hace referencia con un formato similar al de la Constitución Nacional, en su Artículo 43, tratado en el Capítulo 1 de este Trabajo Final de Graduación.

Así, el Artículo 56, reza:

> *Toda persona puede interponer acción de amparo para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos o en los privados destinados a proveer informes y en caso de error, omisión, falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos.* (Constitución de Chubut, 1994)

La provincia de Chubut, con posterioridad, sanciona la Ley 4.244 de Hábeas Data-Protección de Datos Personales, -en 1996- referida a la temática en análisis. La misma tiene por objeto la *"reglamentación del procedimiento de protección de los datos de carácter personal"*, según lo establece el Artículo 1. (Ley 4.244, de Hábeas Data-Protección de Datos Personales, 1996)

Más allá de las coincidencias con las demás leyes provinciales analizadas hasta aquí, esta Ley tiene una particularidad; esto es, no rige respecto de los registros pertenecientes a personas físicas con fines de uso exclusivamente personal, siempre que la información no sea transferida a terceros o difundida; la reproducción de datos ya divulgados en publicaciones oficiales; los datos pertenecientes al sistema de informática jurídica que ya hayan sido publicados en repertorios oficiales.

Esta excepción marca una diferencia sustancial respecto de las constituciones hasta aquí analizadas.

Para finalizar este apartado, dos casos particulares como son la Provincia de La Rioja que contempla el hábeas data expresamente en su constitución, pero no cuenta con una ley específica y, la provincia de Mendoza que, a la inversa que la anterior, ha sancionado una ley referida a la temática, mas no incluye a la figura en su cuerpo normativo máximo.

4.3.7. La Rioja

En lo que respecta a la Constitución de la provincia de La Rioja -reformada en 2002-, refiere a la figura de hábeas data –de manera explícita- en su Artículo 28 bis: *"Toda persona física o jurídica podrá interponer acción de hábeas data para garantizar su derecho de autodeterminación informativa (...)"* (Constitución de La Rioja, 2002) Obsérvese la inclusión del concepto *'autodeterminación informativa'*, el cual podría confrontarse al de la libertad informática, analizado en el Capítulo 1 de este Trabajo Final de Graduación.

En este sentido, la Constitución en análisis agrega que, toda persona:

> *(…) estará facultada para acceder a sus datos personales y los referidos a sus bienes y al destino de tal información que se encuentren asentados en archivos, registros, banco de datos u otros medios técnicos, electrónicos y ópticos, de carácter público o privado, de soporte, procesamiento y provisión de la información (…)*(Constitución de La Rioja, 2002)

Por último, y al igual que las demás analizadas, *"(…) en caso de falsedad o uso discriminatorio de tales datos, exigir la supresión, rectificación, actualización o el sometimiento a confidencialidad de los mismos."* (Constitución de La Rioja, 2002)

En el Artículo 30, la Constitución provincial agrega que: *"(…) la ley preservará el uso de la informática para preservar el honor, la intimidad personal y familiar de los habitantes y el pleno ejercicio de sus derechos."* (Constitución de La Rioja, 2002) En otras palabras, la normativa limitará al uso de la informática para resguardar la intimidad personal y familiar de los habitantes así como también el honor y el pleno ejercicio de sus derechos.

En lo que respecta a los antecedentes penales, por su parte consagra que éstos sólo serán suministrados en los casos previstos por la ley.

4.3.8. Mendoza

Por su parte, la provincia de Mendoza, no menciona expresamente a la figura en su cuerpo normativo máximo pero si, ha sancionado -en el año 2004- la Ley 7.261 de Hábeas Data. Ésta tiene como objetivo crear el Registro de Empresas Privadas de Información de Deudores, definiendo lo que se entiende por empresa privada, en su Artículo 2 Inc. b:

> *(…) b) Será empresa privada de información de deudores: toda persona física o de existencia ideal que suministre, a título gratuito u oneroso, información*

que contenga antecedentes comerciales, financieros y/o bancarios, contenida en archivos, registros, banco o base de datos. (Ley 7.261 de Hábeas Data, 2004)

Más allá de la definición de empresa privada, en el Artículo 3, hace mención a la obligatoriedad de la inscripción de éstas en el Registro mencionado en el párrafo anterior. La función del Registro es controlar el cumplimiento de los requisitos para el suministro de información sensible suministrada por las empresas antes mencionadas. Así como también controlar la calidad y veracidad de información suministrada por las empresas privadas.

De igual manera, establece sanciones para quienes no cumplan con los requisitos y obligaciones impuestas por la presente ley; esto es, -según el caso y la gravedad- apercibimiento, multa, clausura temporaria y definitiva.

Analizando concretamente en lo que refiere a las provincias argentinas en su conjunto, debe considerarse que se advierten algunas carencias, de acuerdo al análisis realizado en sus respectivas constituciones, no así en cuanto a las leyes especiales citadas. Un ejemplo lo conforma la provincia de Córdoba que en el Artículo 50 de su Constitución sólo garantiza el acceso, rectificación y actualización de datos personales, no teniendo en cuenta la confidencialidad y la supresión. De la misma manera, la provincia de La Rioja, novedosamente menciona el derecho de autodeterminación informática adoptando -en tal sentido- la doctrina europea. Finalmente, en la provincia de Buenos Aires, en el Artículo 20 tercer párrafo de su Constitución, sin perjuicio de la mención de la necesidad de una regulación legal, afirma que es una garantía de naturaleza operativa.

De lo expuesto hasta aquí, puede colegirse que, de las constituciones provinciales argentinas analizadas, la constitución de la provincia de Córdoba resulta ser -más allá de alguna carencia específica- una de las más completas en lo que refiere a esta temática, ya que contempla un amplio espectro jurídico, necesario, en lo que a incorporación de los datos personales refiere.

Conclusiones

A lo largo del presente Trabajo Final de Graduación, se ha tratado de dar respuesta al problema planteado; esto es que, si bien el hábeas data es una herramienta de protección y resguardo de los datos personales en Internet, a la fecha, no todas las legislaciones provinciales se adecuan a la Ley 25.326 de Protección de Datos Personales y esto, determina el margen de aplicabilidad en cada una de ellas.

En este sentido, se han organizado los diferentes capítulos que forman parte de este informe, de acuerdo a los objetivos programados. Al llegar a este punto, pueden presentarse las siguientes conclusiones.

Entre los derechos personalísimos, el que refiere a la intimidad, guarde especial relación con la persona y su fuero íntimo. Por esto, el titular de este derecho cuenta con la facultad de oponerse a que su vida se vea afectada por distintas publicaciones que pueden aparece en la Internet o en las redes sociales. La divulgación de datos privados, así como de estados de su vida personal parecen no tener protección alguna cuando de informática se trata. En efecto, el respeto a la vida privada y a la intimidad se constituye como valor fundamental del ser humano y, por esta razón, el mundo del derecho entiende la importancia de tutelarlo y dictar medidas para evitar que sea vulnerado, tanto como para subsanar los daños una vez ocasionados por el uso de la libertad informática.

La doctrina nacional acuerda –desde hace varias décadas- que, el derecho a la privacidad está íntimamente ligado a la libertad informática dada la vulnerabilidad de la persona frente al mal uso de los datos que, una vez almacenados en la Internet, pueden ser utilizados con fines propios o no. En este sentido, los autores citados en el Capítulo 1 hacen referencia a la necesidad de una regulación legal que garantice el derecho de verificar la exactitud, corrección, actualización o reserva de la información.

De allí, surge en la reforma de 1994, la incorporación del Artículo 43 con la figura del hábeas data, dentro del marco de acciones de amparo. Y, al ser incluido para

proteger los derechos constitucionales, eleva –por tanto- la protección de datos personales a la categoría de derecho fundamental, tomando como base las fuentes internacionales donde se contempla este derecho.

El Art. 43 ha tenido en la jurisprudencia, un amplio desarrollo excediendo, de alguna manera, los límites establecidos por dicha norma. Los numerosos casos presentados, las demandas sobre la aplicación del hábeas data frente a los avances tecnológicos y el almacenamiento de datos, hizo que en el año 2000 se dictara la Ley Nº 25.326 de Protección de Datos de Carácter Personal, la que reglamenta la acción del instituto citado.

La Ley 25. 326 de Protección de Datos Personales regula el hábeas data en Argentina y, a la vez, desarrolla y amplía lo consignado por el Artículo 43. La misma, contiene –entre otros- los principios generales relativos a la protección de datos, los derechos de los titulares de datos, las obligaciones de responsables y usuarios de datos, el órgano de control, las sanciones y el procedimiento del recurso judicial hábeas data. Al mismo tiempo, expone los requerimientos para una 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.

Sin entrar en el pormenorizado análisis que se realiza a lo largo del Capítulo 2 y 3 de este Trabajo Final de Graduación referido a la Ley, puede concluirse que, el avance que ha significado la aprobación y puesta en marcha, implica un enorme desafío para el Estado –en cuanto a su cumplimiento y control- y para cada uno de los usuarios de las redes informáticas, dado que el hábeas data sólo es un instrumento rápido y sencillo, cuando –quien demanda sobre el derecho a la privacidad vulnerada- está en conocimiento de los alcances de este instituto.

En este sentido, y como ya se expresara, los aportes analizados desde la jurisprudencia, dan cuenta de cómo su aplicación impulsa a la acción del mundo jurídico sobre la protección de los datos y la aplicación del hábeas data como recurso

más idóneo, advirtiéndose su plena vigencia y aplicación en torno a los damnificados que ven vulnerados su derechos a la privacidad y a la intimidad frente a la libertad informática.

En cuanto al recorrido por los países de Europa, en busca de los aportes del Derecho Comparado, puede observarse un crecimiento relativo con respecto a la legislación. Así cabe destacar a Portugal por haber sido el primero en realizar este reconocimiento expreso en el año 1976. Luego, vendrían varios países europeos y su reconocimiento expreso en su texto constitucional de los derechos de la protección de los datos personales. En otros países –como España- se advierte que, al igual que en Argentina, si bien tienen regulación constitucional, el carácter de esta incorporación es de manera implícita o subyacente dentro de otros derechos reconocidos a lo largo del texto de su ley fundamental. Por último, también se encuentran los Estados en donde no se hace referencia expresa en su legislación constitucional a lo referente a la protección de los datos personales, aunque sin perjuicio a ello, se han dictado normas afines, como es el caso de Francia y Reino Unido.

En los Estados americanos se manifiesta -como carácter común- que la temática referente a los datos personales ha sido incorporada como cláusula constitucional en forma de hábeas data -o como acción de amparo-. Luego vendría la regulación -en leyes especiales- que codifican la materia, sin que sean unánimes las disposiciones referentes a la protección de los derechos vinculados a los datos y su almacenamiento.

Ahora bien, al analizar concretamente lo referido a las provincias argentinas en su conjunto, debe considerarse que se advierten algunas carencias en sus respectivas constituciones, no así en cuanto a las leyes especiales citadas. Como ejemplo, pueden citarse a la provincia de La Rioja que, novedosamente, menciona el derecho de autodeterminación informática adoptando -en tal sentido- la doctrina europea. Mientras que, en la provincia de Buenos Aires, en el Artículo 20 tercer párrafo de su Constitución, sin perjuicio de la mención de la necesidad de una regulación legal, afirma que es una garantía de naturaleza operativa. Finalmente, de las constituciones provinciales argentinas analizadas, la constitución de la provincia de Córdoba resulta ser

-más allá de alguna carencia específica- una de las más completas en cuanto a esta temática, ya que contempla un amplio espectro jurídico, necesario, en lo que a incorporación de los datos personales refiere.

En suma, puede decirse que si bien, la legislación nacional ha avanzado hacia un marco protectivo del derecho a la intimidad, transformando el hábeas data en el mecanismo más idóneo; la realidad en las provincias argentinas es disímil. Y, frente a esta realidad, la vulnerabilidad de las personas y su derecho personalísimo a la intimidad cuando del almacenamiento de datos informáticos se trata, exige la existencia de un marco regulatorio vigente en cada provincia argentina.

Referencias bibliográficas

Doctrina

Bergel, S. D. (1999) *Protección constitucional del derecho a la intimidad a través del hábeas data.* Salvador Darío Bergel. En Chumbita, H. (Coord.) (1999) Nuevos derechos a la información. Instituto Nacional De La Administración Pública. Buenos Aires.

Bidart Campos, G. (1995) *La informática y el derecho de la intimidad.* Ediar. Buenos Aires.

Bustamante Alsina, J. H. (1986) *La protección jurídica de la vida privada frente a la actividad del Estado y las modernas técnicas de la información.* Ediar. Buenos Aires.

Chiovenda, G., (1989) *Instituciones de Derecho Procesal Civil.* Cárdenas editor y distribuidor. México.

Christensen, Eduardo A., (1999) *El hábeas data como tutela en el Derecho Tributario*, Ponencia en el XX Congreso Nacional de Derecho Procesal celebrado del 5 al 9 de oct. 1999 en San Martín de los Andes, Provincia de Neuquén, Libro de ponencias.

Cifuentes, S. (1995) *Derechos personalísimos*. Editorial Astrea. Buenos Aires.

Devis Echandia, H., (1993). *Compendio de derecho procesal*. Biblioteca Jurídica Dike. Colombia.

Diccionario de la Lengua Española (2001) Real Academia Española, Vigésima Primera Edición. Madrid.

Ekmekdjian, Miguel A., (1995) *Tratado de derecho constitucional*, T. III. Depalma. Buenos Aires.

Ferreyra de De la Rúa, A., González de la Vega de Opl, C. (2003) *Teoría general del proceso*. Advocatus. Córdoba.

Frosini, V. (1990), *La protección de la intimidad: de la informática al bien jurídico informático*, en Derecho y tecnología informática, Nº 3, Bogotá.

García San Martín, L. (1995). *Estudio sobre Derecho a la Intimidad.* Editorial Paidós. Buenos Aires.

Gil Domínguez, A. (1999) *La verdad. Un derecho emergente"*. Recuperado el 25 de agosto de 2014. Disponible en www.agdconsultora.com.ar

Gozaini, O. A., (2003) *Ley 25.326 de Protección de Datos Personales*, en L. L. Número especial del suplemento de Derecho Constitucional 150º Aniversario de la Constitución Nacional. Abril.

Moeykens, F. R. (2000) *La protección de datos personales en el proyecto de Código Civil unificado de Comercio de la República Argentina*. Revista en línea. N° 023. Recuperado el 5 de agosto de 2014. Disponible en www.alfa-redi.org.

Organización para la Cooperación y el Desarrollo Económico (OCDE). Recuperado el 5 de agosto de 2014. Disponible en www.ocde.org

Oyarzábal, M. J. A. (2007) *El derecho a la intimidad y el tratamiento de datos personales en el derecho internacional privado argentino.* En Lecciones y ensayos. Departamento de Publicaciones- Facultad de Derecho. Universidad de Buenos Aires. Argentina.

Parellada, C. A. (1990) *Daños en la actividad judicial e informática desde la responsabilidad profesional.* Editorial Astrea. Buenos Aires.

Pérez Luño, A. E. (1990) "*Del habeas corpus" al "habeas data".* Editorial Aranzadi. Madrid.

Pizarro, R. (1991) *Responsabilidad Civil de Los Medios Masivos de Comunicación. Daños por noticias inexactas o agraviantes.* Editor José Luis De Palma. Buenos Aires.

Puccinelli, O. (1999) *El Habeas Data en Indoiberoamérica*. Editorial Temis S. A. Santa Fe de Bogotá, Colombia.

Puccinelli, Oscar R., (1998) *Hábeas data: Aportes para una eventual reglamentación*, en E.D. 161-912. Disponible en www.consejodeabogadoslr.com.ar

Quiroga Lavié, H. y Hernán Lionel Elman, H. L. (2006*) Hacia la verdadera protección. Del derecho a la intimidad.* Revista Iberoamericana de Documentación e Información Judicial. Editorial de la Secretaría Técnica de la Red. Año 2. Número 2. Recuperado el 16 de agosto de 2014. Disponible en www.iberius.org

Rosemberg Holcblat, A. y Sánchez Sanz M. *El derecho a la privacidad en Internet*. Recuperado el 26 de agosto de 2014. Disponible en http://vlex.com/redi/No._37_-_Agosto_del_2001/5

Sagües, Néstor P. (1995) *Derecho Procesal Constitucional, T. 3, Acción de amparo*, 4ta. Edición, Astrea. Buenos Aires

Sagües, P. N. (2007) *Elementos de Derecho Constitucional*. Editorial Astrea. Buenos Aires.

Salazar, E. C. *El Habeas Data en el Derecho Comparado, Edgar Salazar Cano, Anuario Nº 29 (2006), ISSN 1316-5852.* Recuperado el 23 de agosto de 2014. Disponible en www.seriviobc.uc.edu.ve

Santos Briz, J. (1963) *Derecho de Daños.* Editorial Revista de Derecho Privado. Madrid.

Vanossi, J. R., *El hábeas data no puede ni debe contraponerse a la libertad de los medios de prensa*, en *El Derecho*, 13 setiembre 1994 (159-949). Recuperado el 13 de septiembre de 2014. Disponible en www.elderecho.com.ar

Legislación

Constitución de la Nación Argentina.

Ley 25.326 Hábeas Data, Protección de los Datos Personales.

Convenio para la Protección de Personas (1981) Recuperado el 12 de octubre de 2014. Disponible en www.madrid.org

Directiva 95/46/CE. 25 de octubre de 1995. Parlamento Europeo y del Consejo. Recuperado el 12 de octubre de 2014. Disponible en www.eur-lex.europa.eu

Carta de Derechos Fundamentales de la Unión Europea (2000) En Diario oficial de las comunidades europeas (2000) Recuperado el 12 de octubre de 2014. Disponible www.europarl.europa.eu

Castillo Jiménez, C. (1993-1994) Estudio comparativo de la norma 10/91, de Protección de Datos Personales Informatizados, portuguesa y la Ley Orgánica 5/92 de Regulación del Tratamiento Automatizados de los Datos de Carácter Personal (Lortad). Boletín de la Facultad de Derecho, Nº 5, 1993/1994. Sevilla. España. Recuperado el 12 de octubre de 2014. Disponible en www.e-spacio.uned.es

Ley Orgánica 15/99 de Protección de Datos de Carácter Personal, España. Recuperado el 12 de octubre de 2014. Disponible en www.civil.udg.es

Ley 753/78, Francia. Recuperado el 12 de octubre de 2014. Disponible en www.france.fr

Estudio especial sobre el derecho de acceso a la información (2007) Organización de los Estados Americanos. Comisión Interamericana de Derechos Humanos. Relatoría Especial para la Libertad de Expresión. Disponible en www.cidh.oa.org./relatoría/pdf

Ley de Privacidad, (1974), EE.UU. Recuperado el 12 de octubre de 2014. Disponible en www.eeoc.gov

Constitución, 1988, Brasil. En Estudios Constitucionales (2005) Revista Semestral del Centro de Estudios Constitucionales. Universidad de Talca. Chile. Recuperado el 11 de noviembre de 2014. Disponible en www.cecoch.cl

Constitución, 1992, Paraguay. En Estudios Constitucionales (2005) Revista Semestral del Centro de Estudios Constitucionales. Universidad de Talca. Chile. Recuperado el 11 de noviembre de 2014. Disponible en www.cecoch.cl

Constitución Española, 1978. Recuperado el 11 de noviembre de 2014. Disponible en www.derechoshumanos.net

Ley Orgánica de Protección de datos personales (1999) España. Recuperado el 11 de noviembre de 2014. Disponible en www.noticiasjuridicas.com

Constitución, 1993, Perú. En Estudios Constitucionales (2005) Revista Semestral del Centro de Estudios Constitucionales. Universidad de Talca. Chile. Recuperado el 11 de noviembre de 2014. Disponible en www.cecoch.cl

Ley de Hábeas Data 26.301 (1994) Recuperado el 11 de noviembre de 2014. Disponible en www.tc.gob.pe

Ley de Protección de Datos de Carácter Personal, Nº 19.628, Chile. En Estudios Constitucionales (2005) Revista Semestral del Centro de Estudios Constitucionales. Universidad de Talca. Chile. Recuperado el 11 de noviembre de 2014. Disponible en www.cecoch.cl

Ley 18.331, Uruguay. Recuperado el 11 de noviembre de 2014. Disponible en www.parlamento.gub.uy

Muñoz del Alba Medrano, M. (2004) Hábeas data. Recuperado el 11 de noviembre de 2014. Disponible en www.biblio.jurídicas.unam.mx

Ley 17.838 Protección de datos personales para ser utilizados en informes comerciales y acción de habeas data. Recuperado el 11 de noviembre de 2014. Disponible en www.parlamento.gub.uy

Constitución de Córdoba (1986) Recuperado el 27 de noviembre de 2014. Disponible en www.justiciacordoba.gob.ar

Ley 9.380 de Regulación del uso de videocámaras (2007) Recuperado el 27 de noviembre de 2014. Disponible en www.cba.gov.ar

Constitución de Río Negro (1988) Recuperado el 27 de noviembre de 2014. Disponible en www.econ.uba.ar

Ley 3.246 de Acción de Hábeas Data, (1998) Recuperado el 27 de noviembre de 2014. Disponible en www.cpdp.gob.ar

Constitución de Buenos Aires (1994) Disponible en www.hcdiputados-ba.gov.ar, recuperado el 20 de noviembre de 2014

Ley 14.214 de Hábeas data (2010) disponible en www.gob.gba.gov.ar

Constitución de Chaco (1994) Recuperado el 27 de noviembre de 2014. Disponible en www.biblioteca.jus.gov.ar

Ley 4.360 de Hábeas data (1996) Recuperado el 15 de noviembre de 2014. Disponible en www.legislaturachaco.gov.ar

Constitución de San Juan (1996) Recuperado el 27 de noviembre de 2014. Disponible en www.hcdn.gov.ar

Ley 7.447 de Registro público de bancos de datos, (2006) Recuperado el 27 de noviembre de 2014. Disponible en www.cpdp.gob.ar

Constitución de Chubut (1994) Recuperado el 27 de noviembre de 2014. Disponible en www.chubut.gov.ar,

Ley 4.244 de Hábeas data (1996) Recuperado el 27 de noviembre de 2014. Disponible en www.chubut.gov.ar

Constitución de La Rioja (2002) Recuperado el 27 de noviembre de 2014. Disponible en www.larioja.gov.ar

Ley 7.261 de Creación Registro Empresas privadas (2004) Recuperado el 27 de noviembre de 2014. Disponible en www.tribunet.com.ar

Constitución de Mendoza (1989) Recuperado el 27 de noviembre de 2014. Disponible en www.hcdmza.gob.ar

Jurisprudencia

Unión De Usuarios Y Consumidores C/ Citibank S/ Sumarísimo. Buenos Aires, mayo 12 de 2006. Recuperado el 2 de noviembre de 2014. Disponible en www.planetaius.com.ar

M. H. F. C/ BBVA Banco Francés S. A. S/ Habeas Data. Mar del Plata, 22 De Febrero. Recuperado el 2 de noviembre de 2014. Disponible en www.planetaius.com.ar

V. S. H. Recurso de Habeas Data. Expediente Nº 1495-2012. San Nicolás de los Arroyos, 27 de marzo de 2013. Recuperado el 2 de noviembre de 2014. Disponible en www.planetaius.com.ar

AUTORIZACIÓN PARA PUBLICAR Y DIFUNDIR
TESIS DE POSGRADO O GRADO
A LA UNIVERIDAD SIGLO 21

Por la presente, autorizo a la Universidad Siglo21 a difundir en su página web o bien a través de su campus virtual mi trabajo de Tesis según los datos que detallo a continuación, a los fines que la misma pueda ser leída por los visitantes de dicha página web y/o el cuerpo docente y/o alumnos de la Institución:

Autor-tesista *(apellido/s y nombre/s completos)*	Bernardi, Melisa Natalí
DNI *(del autor-tesista)*	33.187.740
Título y subtítulo *(completos de la Tesis)*	**Ley 25.326 de Protección de Datos Personales.** **El derecho a la intimidad y el hábeas data como herramienta de protección y resguardo frente a Internet. Aplicabilidad en las provincias argentinas**
Correo electrónico *(del autor-tesista)*	melisanatalibernardi@hotmail.com
Unidad Académica *(donde se presentó la obra)*	Universidad Siglo 21
Datos de edición: *Lugar, editor, fecha e ISBN (para el caso de tesis ya publicadas), depósito en el Registro Nacional de Propiedad Intelectual y autorización de la Editorial (en el caso que corresponda).*	La Carlota, Melisa Natali Bernardi, Año2016

Otorgo expreso consentimiento para que la copia electrónica de mi Tesis sea publicada en la página web y/o el campus virtual de la Universidad Siglo 21 según el siguiente detalle:

Texto completo de toda la Tesis *(Marcar SI/NO)*[1]	SI
Publicación parcial (informar que capítulos se publicarán)	

Otorgo expreso consentimiento para que la versión electrónica de este libro sea publicada en la en la página web y/o el campus virtual de la Universidad Siglo 21.

Lugar y fecha:

Firma

Aclaración: Melisa Natali Bernardi

Esta Secretaría/Departamento de Posgrado de la Unidad Académica: _ certifica que la tesis adjunta es la aprobada y registrada en esta dependencia.

Firma

Aclaración

Sello de la Secretaría/Departamento de Posgrado

[1] Advertencia: Se informa al autor/tesista que es conveniente publicar en la Biblioteca Digital las obras intelectuales editadas e inscriptas en el INPI para asegurar la plena protección de sus derechos intelectuales (Ley 11.723) y propiedad industrial (Ley 22.362 y Dec. 6673/63. Se recomienda la NO publicación de aquellas tesis que desarrollan un invento patentable, modelo de utilidad y diseño industrial que no ha sido registrado en el INPI, a los fines de preservar la novedad de la creación.