Ratio Iuris
Revista de Derecho
UCES
Vol. 12 Núm. 2, julio-diciembre 2024, pp. 24-35
ISSN: 2347-0151 (en línea)

El impacto del *Big Data* en la protección de datos personales en la legislación argentina

Federico Angel Addati
UCEMA, Ciudad Autónoma de Buenos Aires, Argentina
ORCID: https://orcid.org/0009-0000-9042-746X
Correo electrónico: faddati@gmail.com

Recibido: 12 de septiembre de 2024
Aprobado: 30 de octubre de 2024

Para citar este artículo:
Addati, F. A. (julio-diciembre 2024). El impacto del Big Data en la protección de datos personales en la legislación argentina. *Ratio Iuris, 12*(2), 24-35.
ARK CAICYT: https://id.caicyt.gov.ar/ark:/s23470151/9yzlphq1x

Resumen: Este artículo aborda los desafíos que plantea el uso de *Big Data* en relación con la protección de datos personales en la República Argentina, tomando como referencia la Ley 25.326. Toda vez que el *Big Data* vino a transformar la manera en que se generan y procesan grandes volúmenes de información, surgen importantes tensiones entre la innovación tecnológica y los derechos fundamentales de privacidad. Esta investigación analiza cómo el consentimiento del titular de los datos, siendo este un elemento esencial en la legislación vigente, enfrenta dificultades en el entorno tecnológico del *Big Data*, donde los datos pueden ser reutilizados y compartidos sin que los titulares tengan pleno conocimiento o control. Se identifican limitaciones en la normativa actual que dificultan una protección efectiva frente a las prácticas de recolección y procesamiento masivo de datos. A través de ejemplos concretos, el artículo destaca la necesidad de adaptar y fortalecer el marco legal para responder adecuadamente a los riesgos que impone el *Big Data* en la era digital.

Palabras clave: *Big Data*, tratamiento de datos personales, consentimiento, República Argentina.

Abstract: This article addresses the challenges posed by the use of Big Data in relation to the protection of personal data in the Argentine Republic, taking Law 25,326 as reference. Since Big Data has transformed the way large volumes of information are generated and processed, important tensions arise between technological innovation and fundamental privacy rights. This research analyzes how the consent of the data owner, this being an essential element in current legislation, faces difficulties in the technological environment of Big Data, where data can be reused and shared without the owners having full knowledge or control. Limitations are identified in current regulations that make effective protection against massive data collection and processing practices difficult. Through concrete examples, the article highlights the need to adapt and strengthen the legal framework to adequately respond to the risks imposed by Big Data in the

Ratio Iuris
Revista de Derecho
UCES
Vol. 12 Núm. 2, julio-diciembre 2024, pp. 24-35
ISSN: 2347-0151 (en línea)

digital era.

Keywords: *Big Data, processing of personal data, consent, Argentine Republic.*

Resumo: Este artigo aborda os desafios colocados pelo uso de Big Data em relação à proteção de dados pessoais na República Argentina, tomando como referência a Lei 25.326. Dado que o Big Data transformou a forma como grandes volumes de informação são gerados e processados, surgem tensões importantes entre a inovação tecnológica e os direitos fundamentais de privacidade. Esta pesquisa analisa como o consentimento do titular dos dados, sendo este um elemento essencial na legislação vigente, enfrenta dificuldades no ambiente tecnológico do Big Data, onde os dados podem ser reutilizados e compartilhados sem que os proprietários tenham total conhecimento ou controle. As limitações são identificadas nas regulamentações atuais que dificultam a proteção eficaz contra práticas massivas de coleta e processamento de dados. Através de exemplos concretos, o artigo destaca a necessidade de adaptar e fortalecer o quadro jurídico para responder adequadamente aos riscos impostos pelo Big Data na era digital.

Palavras chave: *Big Data, tratamento de dados pessoais, consentimento, República Argentina.*

Introducción

El entorno tecnológico contemporáneo nos obliga a repensar la manera en que se generan, procesan y utilizan los datos a partir de las interacciones que se dan entre personas, empresas y gobiernos mediante tecnologías y dispositivos conectados a internet. En este contexto, el *Big Dat*a y la Inteligencia Artificial, en adelante IA, han ampliado y transformado significativamente el impacto de esta masiva generación de información.

El *Big Data* permite almacenar y analizar grandes volúmenes de datos provenientes de diversas fuentes, posibilitando identificar patrones y tendencias que serían imposibles de discernir de forma manual. Esta capacidad de procesamiento masivo de información genera conocimientos valiosos, entre otros, sobre comportamientos y preferencias, tanto a nivel individual como colectivo, los cuales pueden ser aprovechados por distintos actores, como empresas y gobiernos.

No obstante, el uso del *Big Data* plantea retos significativos en términos de privacidad y protección de datos personales. En la República Argentina, la Ley 25.326 B.O. 02-11-2000 conocida como Ley de Protección de Datos Personales establece un marco normativo destinado a garantizar el derecho a la privacidad y a regular el tratamiento de la información personal. Sin embargo, la rapidez con que avanzan las tecnologías y el exponencial volumen de datos que se generan día tras día, minuto tras minuto, presenta desafíos que pueden no estar totalmente contemplados en el marco legal actual.

La pregunta de investigación que guía el presente trabajo es la siguiente: ¿en qué medida la Ley 25.326 aborda los desafíos generados por el uso de *Big Data*?

La hipótesis que se trabajará es que la Ley 25.326 resulta insuficiente para enfrentar los desafíos que presenta el uso del *Big Data*.

Ratio Iuris
Revista de Derecho
UCES
Vol. 12 Núm. 2, julio-diciembre 2024, pp. 24-35
ISSN: 2347-0151 (en línea)

Para abordar esta problemática, el trabajo se propone cumplir con los siguientes objetivos específicos:

a) Describir el rol del consentimiento en el tratamiento de datos personales en el contexto del *Big Data* en la República Argentina.
b) Identificar las limitaciones y desafíos que enfrenta el *Big Data* debido a la legislación de protección de datos personales en la República Argentina.
c) Evaluar ejemplos concretos en los que el uso de *Big Data* puede comprometer el consentimiento y otros principios de protección de datos personales en la República Argentina.

La presente investigación resulta relevante en el ámbito jurídico debido a que aborda una de las principales tensiones contemporáneas entre la evolución tecnológica y la protección de derechos fundamentales, como la privacidad y el control sobre los datos personales.

Método

El método que utilizaremos es no experimental. La investigación es descriptiva, básica y documental.

El *Big Data*

La Unión Internacional de Telecomunicaciones (UIT), organismo especializado de las Naciones Unidas para las tecnologías de la información y comunicación (TIC), define el *Big Data* como "un paradigma que permite la recopilación, almacenamiento, gestión, análisis y visualización, potencialmente en tiempo real, de grandes conjuntos de datos con características heterogéneas" (UIT, 2015, párr. 8).

En la República Argentina, la Resolución N° 11-E/2017 de la entonces Secretaría de Tecnologías de la Información y las Comunicaciones creó el Observatorio Nacional de *Big Data*. En esta norma, se utilizan los términos "datos masivos" y "cantidades masivas de datos" para describir al *Big Data*, definido como:

> Conjunto de datos de gran volumen, alta velocidad y/o alta variedad de información, generados a través de la red y mediante el uso de dispositivos inteligentes, que exigen nuevas formas de procesamiento y que incidirán en la toma de decisiones y en la optimización de procesos (Resolución N° 11-E/2017, considerando 6).

Ratio Iuris
Revista de Derecho
UCES
Vol. 12 Núm. 2, julio-diciembre 2024, pp. 24-35
ISSN: 2347-0151 (en línea)

Las características esenciales del *Big Data* son conocidas como las "Vs". Según Irisarri González Deibe (2021), las tres principales "Vs" son Volumen, Velocidad y Variedad de los datos (p. 460). El Volumen se refiere a la enorme cantidad de datos, la Velocidad indica la rapidez con la que estos pueden ser procesados (casi en tiempo real), y la Variedad señala la diversidad de fuentes de datos (Irisarri González Deibe, 2021, p. 460). Posteriormente, se sumaron otras dos "Vs": Veracidad y Valor. La Veracidad se relaciona con la dificultad de asegurar la calidad de los datos debido a su gran volumen, mientras que el Valor refleja el potencial de generar beneficios económicos a partir de estos datos.

Las fuentes de obtención de datos en *Big Data* son diversas, entre ellas, podemos destacar las siguientes:

Dispositivos inteligentes: sensores, relojes, electrodomésticos y vehículos conectados a internet generan grandes cantidades de datos en tiempo real sobre el comportamiento de los usuarios. Además, la popularidad de los *smartphones* y *tablets* permite el acceso constante a internet, registrando el uso de aplicaciones, navegación *web* y datos de geolocalización.

Redes sociales: plataformas como *Facebook, Instagram, Twitter (X)* y *TikTok*, impulsadas por el contenido generado por los usuarios, producen grandes volúmenes de datos sobre preferencias, tendencias y comportamientos, principalmente, a través de imágenes, videos y textos compartidos.

Proveedores de servicios en la nube: empresas como Amazon Web Services (AWS), Google Cloud y Microsoft Azure han facilitado el almacenamiento y procesamiento de enormes cantidades de datos de manera eficiente y escalable.

Plataformas de comercio electrónico y servicios digitales: sitios como *Amazon,* Mercado Libre y servicios de *streaming* como *Netflix, Prime Video, Deezer* y *Spotify* contribuyen significativamente a la generación de datos sobre consumo, patrones de compra y preferencias individuales. Cada transacción, búsqueda o recomendación genera información de valor para empresas y gobiernos.

Administración pública: plataformas digitales en sectores como sanidad y transporte permiten almacenar grandes volúmenes de datos personales de los ciudadanos.

Este procesamiento masivo de información encuentra una restricción -y a la vez, una guía para su aplicación- en la legislación de protección de datos personales, que se desarrollará a continuación.

El derecho a la protección de los datos personales

Los datos personales se encuentran estrechamente vinculados a la existencia de la persona, no solo para identificarla, sino para que la misma pueda ejercer sus derechos y satisfacer sus obligaciones (Masciotra, 2018, p.1).

Ratio Iuris
Revista de Derecho
UCES
Vol. 12 Núm. 2, julio-diciembre 2024, pp. 24-35
ISSN: 2347-0151 (en línea)

En nuestro ordenamiento jurídico, la protección de los datos personales surge del artículo 43 de la Constitución Nacional al prever la garantía del *habeas data* señalando:

> Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos.

Esta garantía fue, posteriormente, reglamentada por la Ley 25.326, Ley de Protección de Patos Personales, en adelante LPDP, y su decreto reglamentario 1558/2001 B.O. .03-12-2001.

La LPDP define a los datos personales como "…la información de cualquier tipo referido a personas físicas o de existencia ideal determinadas o determinables" (artículo 2°). A su vez, describe a los datos sensibles como aquellos que "…revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliaciones sindicales e información referente a la salud o la vida sexual" (artículo 2°).

Por medio de la Ley 27.483 B.O. 2-01-2019 nuestro país incorporó el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal suscripto en la Ciudad de Estrasburgo, República Francesa, el día 28 de enero de 1981 y, por medio de la Ley 27.699 B.O. 30-11-2022, aprobó el Protocolo modificatorio de dicho Convenio, en adelante Convenio. Este trae aparejada nuevas normas que deberán ser interpretadas con la legislación vigente de nuestro país. En particular, resulta dable destacar el artículo 9 el cual señala:

> 1. Cada persona tendrá derecho a:
>
> a) no estar sujeto a una decisión que lo afecte significativamente sobre la base exclusiva de un tratamiento automatizado de datos sin considerar sus opiniones;
>
> b) obtener, cuando así lo solicitare, en intervalos razonables y sin demora o gastos excesivos, confirmación del tratamiento de los datos personales relacionados con su persona, la comunicación en forma inteligible de los datos tratados, toda la información disponible sobre su origen, el periodo de conservación, así como

Ratio Iuris
Revista de Derecho
UCES
Vol. 12 Núm. 2, julio-diciembre 2024, pp. 24-35
ISSN: 2347-0151 (en línea)

> cualquier otra información que el responsable del tratamiento deba proporcionar con el fin de asegurar la transparencia del tratamiento conforme al Artículo 8, párrafo 1 […]
>
> d) oponerse en cualquier momento, por fundamentos relacionados con su situación, al tratamiento de datos personales que lo o la involucren, salvo si el responsable del tratamiento demostrará fundamentos legítimos para el tratamiento superiores a sus intereses o derechos y libertades fundamentales;
>
> e) obtener, cuando así lo solicitare, exento de costos y sin demoras excesivas, la rectificación o eliminación, según sea el caso, de dichos datos si estos estuviesen siendo o hubieren sido tratados en forma contraria a las disposiciones del presente Convenio...

A continuación, nos detendremos a indagar en el consentimiento del titular de los datos personales para analizar cómo impacta con la tecnología del *Big Data*.

El consentimiento como elemento esencial para el tratamiento de datos

En materia de protección de datos, el consentimiento del titular es un elemento esencial para el tratamiento de sus datos personales. El tratamiento se define como las:

> Operaciones y procedimientos sistemáticos, electrónicos o no, que permiten la recolección, conservación, ordenación, almacenamiento, modificación, relación, 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 (artículo 2 LPDP).

En consecuencia, todo banco o registro, público o privado, que desee tratar datos de personas humanas o jurídicas, deberá requerir su consentimiento previo, salvo en los casos excepcionales que señala la ley. Según el artículo 5 de la LPDP, no será necesario el consentimiento cuando:

Ratio Iuris
Revista de Derecho
UCES
Vol. 12 Núm. 2, julio-diciembre 2024, pp. 24-35
ISSN: 2347-0151 (en línea)

a) Los datos se obtengan de fuentes de acceso público irrestricto;

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. (artículo 5 LPDP).

Ahora bien, es fundamental definir las características que deben cumplir el consentimiento. De acuerdo con el artículo 5 de la LPDP:

I. 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…

Cabe señalar que tanto la LPDP como su decreto reglamentario no define qué se entiende por consentimiento “libre” y “expreso”. En cambio, la reglamentación sí lo hizo para el término “informado”.

Es importante determinar el alcance de estos términos, y para ello, recurriremos a Ley 26.994 B.O. 08-10-2014 por la cual se sancionó el Código Civil y Comercial de la Nación, en adelante CCyC, para los dos primeros y luego, para el último, nos ceñiremos a lo que indica el decreto reglamentario de la LPDP.

En torno al consentimiento “libre” desde nuestro punto de vista, se vincula con lo que debe cumplir un acto voluntario, es decir, ser ejercido con intención, discernimiento y libertad conforme lo prevé el artículo 260 CCyC. Por lo tanto, afectará al consentimiento las mismas causales que al acto involuntario, es decir, aquel prestado por falta de discernimiento conforme el artículo 261 del CCyC.

Ratio Iuris
Revista de Derecho
UCES
Vol. 12 Núm. 2, julio-diciembre 2024, pp. 24-35
ISSN: 2347-0151 (en línea)

En cuanto al carácter de "expreso" del consentimiento desde nuestro punto de vista, se entiende que debe ser prestado bajo las formas expresas de manifestación de la voluntad de conformidad con el artículo 262 CCyC. Sin embargo, el legislador en la LPDP privilegió la declaración por escrito, al disponer que el mismo deberá constar de esa forma o por otro medio que permita se le equipare de acuerdo a las circunstancias.

Con respecto a los "medios equiparables", la LPDP da a entender que la modalidad "escrita" no sería excluyente, lo cual da cuenta que podría ser sustituida válidamente según las circunstancias del caso. Aquí es donde toma virtualidad las actuales modalidades electrónicas de prestar el consentimiento, dando, por ejemplo, mediante firma electrónica, un *click* con el *mouse* o con un *touch* en la pantalla de los dispositivos (*Smartphones*, *tables*, pc táctiles, etc).

En consecuencia, es importante destacar que, por ejemplo, en los contratos electrónicos la Cámara de Apelaciones en lo Contencioso Administrativo y Tributario de la Ciudad de Buenos Aires, destacó que cuando un internauta desea ingresar a un sitio *web*, pero que previo a ello, se le exige la aceptación de condiciones generales, al pulsar o cliquear con el botón del *mouse* de la computadora en la leyenda "aceptar" el usuario está expresando su voluntad (CACAyT, Sala I, "AOL Argentina S.R.L. C/ GCBA S/otras causas con trámite directo ante la Cámara de Apelaciones", sentencia de fecha 29-12-2005, voto del Dr. Centenaro).

En relación al consentimiento "informado", la reglamentación indica que es aquel que está precedido al titular de los datos de una explicación adecuada al nivel social y cultural de la información que se tratará (artículo 5 Decreto 1558/01).

Es importante destacar que el consentimiento dado para el tratamiento de datos personales puede ser revocado en cualquier momento. La revocación no tiene efectos retroactivos (artículo 5°, Decreto 1558/01).

Desafíos del *Big Data* en términos de privacidad y consentimiento

Dado que el *Big Data* permite la recolección, almacenamiento y análisis de grandes volúmenes de datos personales de múltiples fuentes, presenta importantes desafíos en cuanto a la privacidad y el consentimiento. Según la LPDP, cualquier entidad que desee tratar datos personales debe obtener una autorización del titular, asegurando que este comprende el alcance de uso de sus datos.

Pero, al utilizarse el *Big Data*, puede verse fácilmente comprometido el consentimiento si la información se obtiene de fuentes de acceso público o si se reutilizan datos previamente recopilados sin actualizar o renovar dicho consentimiento. Dado que se requiere un consentimiento informado, el titular debe recibir información clara, precisa y accesible sobre el uso de sus datos, lo cual puede ser difícil de cumplir en *Big Data*, donde la utilización de los datos evoluciona todo el tiempo. Ejemplos de casos concretos:

Ratio Iuris
Revista de Derecho
UCES
Vol. 12 Núm. 2, julio-diciembre 2024, pp. 24-35
ISSN: 2347-0151 (en línea)

Plataformas de redes sociales y publicidad dirigida:

Redes sociales, por ejemplo, *Facebook*, obtiene el consentimiento de sus usuarios para utilizar su información en la personalización de anuncios. Sin embargo, estos datos también se comparten con terceros para análisis de mercado, sin notificar a los usuarios. La falta de transparencia sobre el destino y el uso final de los datos compromete en cierta forma el consentimiento informado.

Uso de datos de ubicación para análisis de comportamiento:

Una empresa, por ejemplo, de *retail que* recopila datos de ubicación de sus clientes mediante su aplicación móvil para ofrecer promociones en tiempo real puede utilizar también dichos datos para analizar patrones de movilidad urbana sin contar con un consentimiento explícito de los usuarios para este propósito. Esto afecta el consentimiento, ya que estos no están al tanto del uso ampliado de sus datos.

En conclusión, el *Big Data* plantea retos significativos en relación con el consentimiento de los titulares de datos personales, especialmente en términos de transparencia, actualización y revocación de dicho consentimiento.

Otros desafíos que presenta el Big Data en la protección de los Datos Personales

Además de la autorización general para la recolección y tratamiento de los datos, con las excepciones y matices planteados, la LPDP incluye una serie de recomendaciones y obligaciones importantes:

Cambios en la Finalidad del Tratamiento.

La LPDP establece que "los datos objeto de tratamiento no pueden ser utilizados para fines distintos o incompatibles con aquellas que motivaron su obtención" (artículo 4.3 LPDP).

Ejemplo:

En un sistema de *Big Data*, una empresa que recolecta datos de sus clientes con el fin de ofrecer recomendaciones personalizadas de productos podría después usar esta información para investigaciones de mercado y estudios demográficos sin notificar ni obtener un nuevo consentimiento de los usuarios. Esto implica un cambio en la finalidad que podría ir en contra de la LPDP.

Calidad de la Información.

La LPDP establece que los datos deben ser "ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenidos" (artículo 4.1 LPDP).

Ratio Iuris
Revista de Derecho
UCES
Vol. 12 Núm. 2, julio-diciembre 2024, pp. 24-35
ISSN: 2347-0151 (en línea)

Además, el titular de los datos tiene derecho a acceder, corregir y suprimir la información (artículos 13, 14 y 16 LPDP).

Ejemplo:

En un contexto de *Big Data*, los datos se obtienen de múltiples fuentes, lo que aumenta el riesgo de errores, duplicación de información y datos desactualizados. Así, un banco que utiliza *Big Data* para evaluar el riesgo crediticio de los clientes podría tener problemas si utiliza datos incorrectos o incompletos, afectando las decisiones financieras de sus clientes y violando el principio de calidad de la información.

Obligación de Seguridad de la Información y Confidencialidad para los Agentes que Hacen el Tratamiento.

La LPDP prohíbe la creación de registros en bases de datos que "no reúnan condiciones técnicas de integridad y seguridad" (artículo 9 LPDP).

Ejemplo:

Las grandes cantidades de datos recopilados y almacenados en plataformas de *Big Data* suelen ser atractivos para ataques cibernéticos. Una empresa de telecomunicaciones que almacena datos de ubicación y uso de sus clientes podría ser víctima de una filtración si no implementa las medidas de seguridad adecuadas, exponiendo datos confidenciales y comprometiendo la seguridad y privacidad de los titulares.

Conclusiones

En mérito de todo lo expuesto, podemos concluir que la presente investigación ha permitido analizar los desafíos que plantea el *Big Data* en el contexto de la protección de datos personales en Argentina, especialmente en relación con la Ley 25.326.

En cuanto al rol del consentimiento en el tratamiento de datos personales, se ha destacado que, aunque la LPDP establece la necesidad de un consentimiento libre, expreso e informado, el entorno de *Big Data* dificulta su aplicación en la práctica debido a la naturaleza evolutiva y reutilizable de los datos. Esto plantea una tensión entre el consentimiento inicial otorgado y los nuevos usos que se pueden dar a los datos sin conocimiento del titular, afectando la transparencia y la capacidad de revocación.

Asimismo, se han identificado limitaciones en la legislación actual, como su falta de adaptación a la recolección masiva y al procesamiento automatizado de datos que caracterizan al *Big Data*. Aunque la LPDP establece principios claros sobre la calidad y seguridad de la información, así como la limitación en la finalidad del tratamiento, la práctica de *Big Data* tendería a desafiar estos principios, dado que los datos se recolectan de múltiples fuentes y se utilizan en contextos diversos. Esto conlleva a aumentar el riesgo de errores y el uso de información desactualizada o inexacta.

Por último, hemos ofrecido casos específicos que ilustran cómo el *Big Data* puede comprometer el horizonte trazado por la LPDP. Si bien esta proporciona una base importante para la protección de datos personales, resulta insuficiente para enfrentar los desafíos del *Big Data*, lo que sugiere la necesidad de actualizar el marco legal para adecuarlo a las realidades tecnológicas actuales.

Referencias bibliográficas

Cámara de Apelaciones en lo Contencioso Administrativo y Tributario de la Ciudad Autónoma de Buenos Aires, Sala I, 29-12-2005, "AOL Argentina S.R.L. c/ GCBA s/otras causas con trámite directa ante la Cámara de Apelaciones", *La Ley AR/JUR/13804/2005*

Decreto Reglamentario 1558/2001. Reglamentación ley 25.326. https://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70368/texact.htm

Irisarri González Deibe, N. (2021). Big Data en salud: Beneficios y riesgos en Argentina. *Ratio Iuris, Revista de Derecho Privado, 9(2),* 455-475.

Ley 25.326. Régimen legal del Habeas Data. http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=64790

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

Ley 27.483. Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. https://servicios.infoleg.gob.ar/infolegInternet/anexos/315000-319999/318245/texact.htm

Ley 27.699. Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. https://servicios.infoleg.gob.ar/infolegInternet/anexos/375000-379999/375738/norma.htm

Masciotra, M. (2018). Protección de datos personales y su integración en el marco de los derechos humanos. *Sistema Argentino de Información Jurídica, DACF 180264*

Resolución E 11/2017. Creación del Observatorio Nacional de Big Data. https://servicios.infoleg.gob.ar/infolegInternet/anexos/275000-279999/275597/norma.htm

Unión Internacional de Telecomunicaciones (2015). Los Miembros de la UIT acuerdan una norma internacional para los grandes volúmenes de datos (Big Data). Aprovechar la computación en la nube para prestar servicios de Big Data. Comunicado de prensa. https://www.itu.int/net/pressoffice/press_releases/2015/66-es.aspx