



FACULTAD DE DERECHO Y CS. JURÍDICAS

TRABAJO FINAL DE GRADO

TÍTULO: “Perfilamiento digital. El límite a la recopilación de datos biométricos.”

Alumna: Florencia Belen Suriano

Legajo N°: 6218

Tutor: Prof. Mg. Gabriel E. Lanzavechia.

Título al que aspira: Abogada.

Facultad de Derecho y Ciencias Políticas

Carrera: Abogacía.

Fecha de presentación: 25/08/2023

Teléfono: 1165119460

Correo electrónico: Florenciasuriano1993@gmail.com

Localización: Centro

Abstract.

El presente trabajo de investigación tiene por objeto comprobar que la normativa vigente en Argentina en materia de datos personales es insuficiente.

Se elaboró una hipótesis afirmando la necesidad de regulación más estricta en el ámbito del tratamiento de datos personales.

Para corroborar la hipótesis se ha analizado teóricamente la normativa vigente y se ha llevado a cabo una encuesta sobre Perfilamiento Digital, que comprueba que la sociedad se encuentra en desventaja y desprotegida frente al tratamiento masivo de datos.

Como propuesta se sugiere mayor intervención por parte del Estado, la sanción del Proyecto de Ley de Datos Personales y la creación de normas que incluyan la problemática sobre perfilamiento digital y datos biométricos.

Palabras clave.

Inteligencia Artificial. Derechos personalísimos. Derecho a la imagen. Derecho a la privacidad. Ley de propiedad intelectual. Datos personales. Datos biométricos. Habeas data. Intimidad. Actos personalísimos. Consentimiento. Perfilamiento digital. Redes sociales. Big Data. Machine Learning. Deep Learning. Derecho de Acceso a la Información Pública. Medidas Autosatisfactivas. Medidas Cautelares. Perfilamiento Digital. Datos genéticos. Datos Personales Sensibles

Índice

Agradecimientos.....	5
Solicitud de Tutoria.....	6
Aceptacion.....	7
Notas administrativas.....	8
Reserva de tesis y designación de tutor.....	9
Capitulo I. Introducción.....	10
Capitulo II.- Planteo del problema jurídico relevante.....	11
Capitulo III.- Hipotesis.....	18
Capitulo IV.- Marco Teórico Filosófico y general.....	19
IV.1.- Objetivos del trabajo de Investigación.....	19
IV.1.A).-Objetivos generales.....	19
IV.1.B.- Objetivos Especificos.....	20
IV.2.- Metodología.....	20
Capitulo V.- Marco Teórico Específico.....	22
V.1 Marco normativo.....	22
V. 2 Nuevo Proyecto de Ley de Protección de Datos Personales.....	24
Principales modificaciones.....	24
Ámbito de aplicación material y territorial.....	26
Principios.....	26
Consentimiento y revocación.....	27
Información al titular de los datos.....	27
Tratamiento de datos sensibles.....	27
Tratamiento de datos del sector público.....	28
Tratamiento de datos de niñas, niños y adolescentes.....	28

Principio de seguridad de los datos personales y notificación de incidentes.....	29
Deber de confidencialidad.....	29
Transferencias Internacionales.....	29
Derecho de los titulares de los datos.....	30
Ejercicio de los derechos y excepciones.....	31
Obligaciones de los responsables y encargados del tratamiento.....	32
Protección de información crediticia y derecho al olvido.....	34
Ámbito de aplicación.....	34
Procedimientos y sanciones.....	34
Acción de Habeas Data.....	35
Legitimación activa y pasiva.....	35
Competencia.....	35
Admisibilidad y procedimiento:.....	36
Sentencia.....	36
V.3.- Perfilamiento digital.....	37
V.4.- ¿Que son los datos biométricos?.....	38
V.5.- Fallos nacionales.....	40
V.6.- Derecho comparado.....	42
Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108) – UE	42
Reglamento General de Protección de Datos – UE (RGPD).....	42
Estándares de protección de datos personales de la red Iberoamericana de Protección de Datos (RIPD).....	43
Principios actualizados sobre la privacidad y la Protección de Datos Personales – OEA.....	43

Recomendación sobre la Ética de la Inteligencia Artificial UNESCO.....	43
Ley General de Protección de Datos (LGPD) – Brasil.....	43
Ley Orgánica de Protección de Datos Personales - Ecuador.....	43
Capítulo VI.- Investigacion.....	44
VI. 1.- Análisis e interpretación de resultados.....	44
Capitulo VII .- Conclusión.....	52
Capitulo VIII.- Propuesta.....	53
Bibliografía.....	54

AGRADECIMIENTOS

A mi hijo Vittorio, por acompañarme en esta pasión que es para mí el Derecho y ser mi motivación para ser mejor persona y profesional cada día.

A mi familia, Micaela, Patricia y Eduardo, por ayudarme a cumplir este sueño.

A mis compañeros de facultad y amigos, por todos los momentos compartidos.

A mi tutor, Dr. Gabriel Lanzavechia, por guiarme en este camino, por la dedicación con cada uno de sus alumnos y por impulsarnos a siempre mejorar, pero por sobre todo, gracias por la comprensión.

A la Universidad Abierta Interamericana por permitirme estudiar y cumplir un sueño, transitando este largo pero hermoso camino junto a grandes profesores y personas que conocí, de todos he aprendido algo.

SOLICITUD DE TUTORÍA PARA TESIS.

Buenos Aires, 21 de Diciembre de 2021.-

Estimado Prof. Dr. Gabriel Lanzavechia:

Me dirijo a usted por medio de la presente a fin de solicitarle su ayuda como tutor para la confección de mi trabajo final.

El título del mismo será: *“Perfilamiento digital. El límite a la recopilación de datos biométricos.”*

Asimismo, declaro conocer expresamente los recaudos dispuestos por el **Resolución C.S. N° 1102/2022 U.A.I.** para la confección de trabajos finales, y asumo la responsabilidad de desempeñar el desarrollo del presente trabajo de investigación conforme las pautas metodológicas dispuestas por mi tutor siendo las mismas de tipo orientativas; como así también bajo la experticia adquirida como alumna en el marco de las materias dictadas por la Universidad Abierta Interamericana. Declaro bajo juramento que el trabajo de investigación a confeccionar resultará pura y exclusivamente obra intelectual de la Suscripta, asumiendo la responsabilidad civil y/o penal de la autoría intelectual de la obra a desarrollar, liberando al Prof. Mg. Gabriel E. Lanzavechia de cualquier consecuencia jurídica devenida del presente trabajo.

Desde ya muchas gracias.

Saludos cordiales.

ALUMNO: Suriano Florencia Belen

LEGAJO: 6218

ACEPTACIÓN DEL CARGO POR EL TUTOR

De mi mayor consideración:

Por la presente comunico a Ud. que acepto desempeñarme como tutor del Trabajo Final de la alumna **Florencia Belén Suriano**

Declaro conocer la reglamentación vigente.

No asumo responsabilidad penal y/o civil por la presente obra, toda vez que la producción integral de la misma resultará exclusiva propiedad intelectual de la tesista; siendo el carácter de las instrucciones realizadas por el Suscripto, opiniones meramente metodológicas y orientadoras del área de incumbencia del trabajo de investigación.-

Prof. Gabriel E. Lanzavechia

NOTAS ADMINISTRATIVAS



Gabriel E. Lanzavechia <lanzavechia@gmail.com>
Jue 18/11/2021 3:43
Para: Suriano, Florencia Belen
CC: Miceli, Marilina <Marilina.Miceli@UAI.edu.ar>; Lanzavechia, Gabriel Eduardo <Gabriel.Lanzavechia@UAI.edu.ar>
Confirmo tutoría
...



Suriano, Florencia Belen
Jue 18/11/2021 3:40
Para: Miceli, Marilina <Marilina.Miceli@UAI.edu.ar> y 2 más
Estimada Marilina,
cómo te había comentado, deseo cambiar el tema de tesis que había reservado: "Marco Normativo de los Recursos Hídricos".
El nuevo tema de tesis que voy a presentar es "Inteligencia Artificial y Responsabilidad Civil".
Mi idea es presentarla en Febrero y defenderla en Marzo.
Copio al Dr. Lanzavechia que es mi tutor.
Muchas gracias.
Saludos cordiales

RESERVA DEL TEMA DE TESIS Y DESIGNACIÓN DE TUTOR.



Suriano, Florencia Belen

Jue 16/12/2021 9:30

Para: Gabriel E. Lanzavechia <lanzavechia@gmail.com>; Miceli, Marilina <Marilina.Miceli@UAI.edu.ar>

 introduccion tesis suriano flo...

141 KB

Estimada Marilina,

En relación a los mails anteriores, adjunto breve introducción sobre el contexto normativo del tema que quiero reservar, si bien habla sobre inteligencia artificial y responsabilidad civil (es un campo de estudio muy amplio para investigar), mi trabajo está enfocado particularmente a los vehículos automatizados.

Aguardo confirmación y copio a mi tutor Dr. Lanzavechia Gabriel.

Muchas gracias





Gabriel E. Lanzavechia <lanzavechia@gmail.com>

Jue 16/12/2021 9:33

Para: Suriano, Florencia Belen

CC: Miceli, Marilina <Marilina.Miceli@UAI.edu.ar>

Estimada Marilina,

Quedamos al aguardo de saber si el tema y la modalidad es viable.

Aguardamos comentarios.



Prof. Mg. Gabriel E. Lanzavechia.

TEMA DE TESIS FLORENCIA BELEN SURIANO DNI: 38.010.239

 1 



Miceli, Marilina <Marilina.Miceli@UAI.edu.ar>

Jue 16/12/2021 11:00

Para: Gabriel E. Lanzavechia <lanzavechia@gmail.com>; Suriano, Florencia Belen

Tema registrado. Atte

Get [Outlook para Android](#)

CAPÍTULO I -

INTRODUCCIÓN.

La sociedad avanza y cambia rápidamente con la aparición de las nuevas tecnologías. Estas tienen múltiples objetivos y prometen facilitar las acciones de la vida diaria y realizar tareas por el humano en un tiempo record, como es el caso de la recolección de datos mediante la Inteligencia Artificial (en adelante IA), que ha demostrado ser una herramienta poderosa para el análisis y la toma de decisiones en una amplia variedad de campos, desde la atención médica hasta el sistema de seguridad. Sin embargo, su uso también ha planteado cuestiones críticas en torno a la privacidad, la transparencia y la responsabilidad.

Casi de manera automática, contamos con la colaboración de la IA en las acciones que realizamos a diario, desde el uso del GPS que nos brinda el camino más rápido a un destino predeterminado, analizando el tráfico y las condiciones climáticas en cuestión de segundos, hasta las recomendaciones que nos brindan las Apps según nuestros gustos y preferencias.

Estos avances tecnológicos que se presentan tan precipitadamente, traen consigo aspectos favorables ya que simplifican acciones y optimizan nuestro tiempo, pero también tienen su aspecto negativo que despiertan ciertas preocupaciones, por lo que el derecho debe de estar a la altura para poder brindar soluciones a los nuevos problemas que se plantean. Y es que, la tecnología en términos de IA puede ser muy útil pero no deja de representar una amenaza para el ser humano, puntualmente en lo que respecta al presente trabajo de investigación, la recopilación y el uso de datos personales por parte de los sistemas de IA pueden ser invasivos y comprometer la privacidad y la seguridad de las personas. Por estas razones, es importante crear un marco de seguridad jurídica en el desarrollo y la implementación de la IA en nuestra sociedad, para garantizar su uso responsable y sostenible en beneficio de todos.

En conclusión, la relación entre la IA y el derecho en Argentina es esencial para garantizar el uso responsable y sostenible de esta tecnología. Esto requiere de una regulación adecuada y actualizada que permita proteger los derechos fundamentales de las personas.

CAPÍTULO II –

PLANTEO DEL PROBLEMA JURÍDICO RELEVANTE.

Desde el momento en que nacemos, toda nuestra existencia se encuentra registrada, hasta nuestra muerte. Esta información se almacena en bancos de datos públicos y privados, y es información estrictamente relacionada con la intimidad de las personas, como pueden ser orientaciones políticas, sexuales, religión, enfermedades, si no se tratan adecuadamente el resultado puede ser discriminatorio y/o violatorio de los derechos personalísimos.

Es así que utilizamos nuestros teléfonos celulares o automóviles que incluyen GPS para llegar más rápido a nuestro destino, de la misma forma que le pedimos a Siri (asistente personal de Apple que cuenta con personalidad propia dotada de IA) en la búsqueda de inmediatez y optimización de nuestro tiempo, también estamos brindando múltiples datos que se almacenan en la inmensidad de la internet sin dimensionar el efecto que tienen los mismos ni las consecuencias.

Todos esos datos que brindamos, son recopilados por la IA con distintos objetivos dependiendo de cada empresa o mismo del Estado, y con ellos se va generando un “perfil digital” de cada individuo, no solo con nuestros rasgos físicos sino también con datos sensibles o nuestras preferencias, inclusive la manera en la que nos relacionamos con los demás a través de las redes sociales, así es que somos perfilados digitalmente, sin consentimiento y en la mayoría de los casos sin siquiera saberlo.

Ahora bien, es necesario hacer una breve reseña para conocer cómo se fue adaptando nuestra legislación en materia de tratamiento de datos personales:

Primeramente, nuestra ley fundamental reconoce el derecho a la protección de datos personales en su art. 43: *“Toda persona puede interponer acción expedita y rápida de amparo, siempre que no exista otro medio judicial más idóneo, contra todo acto u omisión de autoridades públicas o de particulares, que en forma actual o inminente lesione, restrinja, altere o amenace, con arbitrariedad o ilegalidad manifiesta, derechos y garantías reconocidos por esta Constitución, un tratado o una ley. En el caso, el juez podrá declarar la inconstitucionalidad de la norma en que se funde el acto u omisión lesiva.”*

Argentina fue el primer país en América Latina en crear una ley destinada al tratamiento de datos personales (LPDP), sancionada en el año 2000, reglamentada en el año 2001 por el Decreto N° 1558 y declarada por la Unión Europea como “legislación adecuada” en protección de datos personales, como lo establece su Art. 1, tiene por objeto la protección integral de aquellos datos personales que se encuentran asentados en archivos, registros, cualquier medio que pueda utilizarse para el tratamiento de datos, con el fin de que no se vulneren derechos personalísimos y el acceso que deben tener todos los individuos a la información que se registre sobre sí mismos.

El régimen de protección de datos tiene como objetivo regular la capacidad de las personas para gestionar o suprimir datos sobre sí mismas y, por otro lado, mediante un conjunto de normas específicas y principios generales, establecer límites al uso de los datos tanto de entidad pública como privada.

En el año 2018, Argentina se adhirió al Convenio para la Protección de Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (más conocido como Convenio 108+), tratado internacional que establece normas y principios para la protección de la privacidad y los derechos de las personas en relación con el tratamiento automatizado de datos personales.

El Estado y las empresas utilizan el tratamiento de datos como un método de control, y también como una estrategia de publicidad, análisis de mercado y otros fines comerciales, es así que nos encontramos ante la necesidad de crear normas que generen un marco de seguridad al usuario, actualmente no hay regulación específica que este a la altura de la revolución tecnológica que estamos atravesando ya que la normativa con la que contamos, no contempla el peligro respecto de la recopilación de los datos biométricos y no considera por ejemplo, el derecho a no ser perfilado, esta circunstancia puede ocasionar múltiples perjuicios relacionados con la violación a la privacidad o discriminación, ante esta necesidad imperante de actualizar la ley de datos personales, la Agencia de Acceso a la Información Pública(AAIP)¹ inició un proceso de debate y como resultado de ese proceso, se presentó un Nuevo Proyecto de Ley de Protección de Datos Personales, si bien su modificación supone un gran avance, lo cierto es que la misma no abarca cuestiones como el problema del perfilamiento digital que ya he mencionado, es por ello que nace el problema jurídico relevante del presente trabajo de investigación: **¿Cuál es el límite a la recopilación de datos biométricos?**

¹ La Agencia de Acceso a la Información Pública (AAIP) es, a partir del 17 de septiembre de 2017, la autoridad de aplicación de la Ley de Protección de Datos Personales.

La Unión Europea en su nuevo reglamento destinado a la protección de datos personales en su Art.4² define a los datos biométricos como *“Aquellos datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos”*. El Nuevo Proyecto de Ley de Protección de Datos Personales, en su Art.2 adopto la misma definición.

Los datos biométricos están estrictamente relacionados con la identidad, ya que mediante ellos se identifica inequívocamente a una persona, también con la privacidad, ya que los datos biométricos son datos sensibles, los titulares de esos datos tienen derecho al consentimiento informado, es decir, a saber cómo se están utilizando sus datos y brindar el consentimiento para su uso, es muy importante que el procedimiento respete el marco legal, ya que los datos biométricos proporcionan detalles íntimos del cuerpo humano, y su naturaleza permanente impide que, en caso de una utilización ilegítima, se pueda reparar el daño causado. A diferencia de una contraseña, no podemos crear una nueva huella digital o imagen facial.

En el sector público, la ANSES utiliza el sistema de datos biométricos denominado Mi Huella, *es un sistema que permite reconocer la identidad de las personas a través de la digitalización de las huellas dactilares para facilitar la realización de trámites. En algunos casos puede solicitarse la exención.*³ Asimismo, la AFIP también utiliza los datos biométricos para validar la identidad de los contribuyentes, mediante la app Mi Afip los datos que se solicitan son: firma, foto, huella dactilar y Documento Nacional de Identidad (DNI) escaneado, y según la web de AFIP la finalidad del sistema es *“Para una identificación más segura con el fin de evitar la utilización de documentación apócrifa y preservar la seguridad jurídica y patrimonial de las personas ajenas a la comisión de dichos fraudes.”*⁴

² REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO- 27/04/2016

³Exención de Mi Huella. <https://www.anses.gob.ar/jubilaciones-y-pensiones/consultas-y-tramites-frecuentes-para-jubilados/registro-de-mi-huella/exencion-de-mi-huella#:~:text=Mi%20Huella%20es%20un%20sistema,casos%20puede%20solicitarse%20la%20exenci%C3%B3n>. Consultado: 04/05/2022

⁴ Datos Biométricos. https://servicioscf.afip.gob.ar/publico/abc/ABCpaso2.aspx?id_nivel1=2949&id_nivel2=3138&p=Datos%20Biom%C3%A9tricos#:~:text=Los%20datos%20biom%C3%A9tricos%20deben%20registrarse,la%20comisi%C3%B3n%20de%20dichos%20fraudes. Consultado: 04/05/2022

Lo cierto es que tanto en el ámbito privado como público, las Apps como programas de software deben cumplir con ciertos requisitos en concordancia con la Ley 25.326 que brinden al titular de los datos el control de los usos que se le dará a su información, toda vez que *“El dato, sin importar donde se encuentre almacenado, siempre es propiedad de su titular.”*⁵ Quien se encarga de controlar que se dé cumplimiento con la LDDP es la Dirección Nacional de Protección de Datos Personales (DNPDP).

¿Qué derechos se encuentran comprometidos ante el uso indebido en el tratamiento de datos?

Derechos Personalísimos: Son aquellos derechos inherentes al ser humano que parten del valor fundamental del respeto por la persona humana y son inalienables, si bien al momento de crearse la ley 25.326 estos derechos se encontraban contemplados en la Constitución y Tratados Internacionales, luego de 13 años, fueron incluidos también en el Nuevo Código Civil y Comercial, en el Capítulo 3 del Título I “Derechos y actos personalísimos”, allí se incorpora el concepto de “dignidad” como punto de partida, de ella derivan todos los derechos de la personalidad, Art. 51 CCCN: *“Inviolabilidad de la persona humana. La persona humana es inviolable y en cualquier circunstancia tiene derecho al reconocimiento y respeto de su dignidad.”* Es decir, que todos los seres humanos merecen ser tratados con igualdad, y de gozar de los derechos fundamentales que derivan de la propia existencia del ser humano.

Derecho a la imagen.

En el año 1933 se creó la Ley N° 11.723 Régimen Legal de la Propiedad Intelectual, su Art. 31 se refiere al registro fotográfico y dispone: *“El retrato fotográfico de una persona no puede ser puesto en el comercio sin el consentimiento expreso de la persona misma y muerta ésta, de su cónyuge e hijos o descendientes directos de éstos, o en su defecto, del padre o de la madre. Faltando el cónyuge, los hijos, el padre o la madre, o los descendientes directos de los hijos, la publicación es libre. La persona que haya dado su consentimiento puede revocarlo resarciendo daños y perjuicios. Es libre la publicación del retrato cuando se relacione con fines científicos, didácticos y en general culturales, o con hechos o acontecimientos de interés público o que se hubieran desarrollado en público.”*

⁵ GUIA DE BUENAS PRACTICAS EN PRIVACIDAD PARA EL DESARROLLO DE APLICACIONES - Dirección Nacional de Protección de Datos Personales (Microjuris Cita: MJ-LEG-70425-90001-AR | LEG70425)

Dicho artículo regula los límites y prohibiciones a la publicación del registro fotográfico, siendo el pilar fundamental para realizar dicho acto, el consentimiento, hoy en día existen en la sociedad diversos medios capaces de captar y reproducir la imagen personal (incluida la voz de la persona también) , por tal motivo, ya no alcanzaba solo con mencionar el “retrato fotográfico”, y si bien dicho Art. sigue vigente y sigue siendo útil, fue necesario incorporar nuevas normas que se adapten a otros medios posibles capaces de reproducir la imagen personal.

Es así que con la llegada del Nuevo código civil y comercial, se incorporó el art. 53 que dispone: *“Derecho a la imagen. Para captar o reproducir la imagen o la voz de una persona, de cualquier modo que se haga, es necesario su consentimiento, excepto en los siguientes casos: a. que la persona participe en actos públicos. que exista un interés científico, cultural o educacional prioritario, y se tomen las precauciones suficientes para evitar un daño innecesario; c. que se trate del ejercicio regular del derecho de informar sobre acontecimientos de interés general. En caso de personas fallecidas pueden prestar el consentimiento sus herederos o el designado por el causante en una disposición de última voluntad. Si hay desacuerdo entre herederos de un mismo grado, resuelve el juez. Pasados veinte años desde la muerte, la reproducción no ofensiva es libre”*.

Aquí se contempla todos los medios que en la actualidad pueden captar y reproducir la imagen como pueden ser medios auditivos, visuales o audiovisuales, es por ello que se incluye la voz y se hace referencia a cualquier registro que posibilite identificar a la persona.

También refiere a dos acciones diferentes, por un lado tenemos la acción de captar y por otro lado la acción de reproducir, para ambas acciones es necesario el consentimiento de la persona, esto quiere decir, que podemos dar consentimiento para captar y no para reproducir, o al revés.

Podemos concluir entonces, que el derecho a la imagen es un derecho personalísimo, ya que se encuentra comprendido dentro de los límites de la voluntad y de la autonomía privada del individuo y, de igual manera sucede con el tratamiento de datos personales, como lo dispone el Art. 5⁶ de la ley Ley 25.326 el tratamiento de datos

⁶ ARTICULO 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) Se recaben para el ejercicio de

personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado.

Toda persona tiene sobre su imagen un derecho exclusivo que se extiende a su utilización de modo de poder oponerse a su difusión cuando ésta es hecha sin autorización, a menos que se den circunstancias que tengan en miras un interés general que aconseje hacerlas prevalecer sobre aquel derecho. La producción de este derecho es independiente de la tutela al honor, a la intimidad y a la privacidad (Sala H, 15/4/2004 “Bocanera, Orlando c. Diario Clarín y otro”).

Por último, se destaca que el Derecho a la Imagen se encuentra reconocido en tratados Internacionales, como la Declaración Americana de los Derechos del Hombre (art. 5), Pacto de San José de Costa Rica (art. 11) y Pacto Internacional de Derechos Civiles y Políticos (art. 17).

Derecho a la Intimidad:

La intimidad sugiere, el reconocimiento de una esfera de vida personal exclusiva, de un sector de la persona que le es propio y que puede excluir del acceso de terceros. Es extremadamente amplio y variado el conjunto de manifestaciones que comprende, y es complejo elaborar reglas generales y un catálogo enunciativo de todas ellas. Su delimitación y su contenido son relativos, pues dependen de la persona (pública o privada) y de las circunstancias de cada caso concreto. Esto último, incluso, según el propio modo de ser y del querer del titular, en el sentido de que ello determinará el ámbito de su intimidad acorde con su particular idiosincrasia, sus necesidades o aspiraciones y el interés personal en una mayor o menor reserva (Tobías, José W., *Derecho de las personas, La Ley, Buenos Aires, 2009, p. 657 y ss.*).

La tutela de este derecho encuentra su primera consagración en el art. 19 de nuestra Carta Magna, que expresamente ampara la intimidad de las personas, conjuntamente con una serie de tratados internacionales (art. 12 de la Declaración Universal de Derechos Humanos, art. 11 incs. 2 y 3 de la Convención Americana de Derechos Humanos, art. 17 del Pacto de Derechos Civiles y Políticos).

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.

De lo expuesto anteriormente, damos cuenta de la importancia de contar con una normativa en protección de datos personales, que se encuentre a la altura de la gran problemática relacionada con la privacidad y seguridad, ya que la información recopilada podría ser utilizada para fines malintencionados, como el robo de identidad.

Es por ello, que el 9 de noviembre de 2022 el Congreso de la Nación aprobó el Convenio 108+ que modifica al Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal N° 108, en dicha reforma se amplió el concepto de dato sensible, agregando a esa definición los datos genéticos y biométricos, entre otras cosas.

CAPÍTULO III –

DEL PLANTEO DE HIPÓTESIS.

La capacidad de recopilar, almacenar y analizar grandes cantidades de datos es un avance tecnológico que, como ya hemos visto, se encuentra estrictamente relacionada con derechos fundamentales como la intimidad y la privacidad, lo que supone un peligro para la seguridad de la información personal.

La inseguridad cibernética, la recopilación o uso indebido de datos han desencadenado debates sobre cómo equilibrar la innovación tecnológica con la necesidad de proteger los derechos de las personas.

Por lo expuesto, se formula en grado de hipótesis que:

“Una regulación normativa más estricta en el ámbito del tratamiento de datos personales, incluyendo datos biométricos y mayor información para los titulares de datos, proporcionará un marco sólido de seguridad jurídica que garantice el adecuado tratamiento y almacenamiento de dichos datos. Esta regulación deberá abordar el derecho del individuo a tomar decisiones sobre su “perfilamiento digital”, brindándole la información clara y fácil de entender, al mismo tiempo que establece límites claros que preserven los intereses tanto del titular de los datos como del responsable del tratamiento.”

CAPÍTULO IV -

MARCO TEÓRICO FILOSÓFICO Y GENERAL

El derecho es una disciplina en constante evolución, que se debe adaptar a los cambios y necesidades de la sociedad, se busca probar en el presente trabajo la necesidad de la actualización y aplicación de normas legales específicas, en lugar de consideraciones subjetivas sobre lo que es éticamente correcto.

Hans Kelsen, creador de “La Teoria Pura del Derecho” ubica al Derecho como un fenómeno autónomo de consideraciones ideológicas o morales, del cual excluyó cualquier idea de “derecho natural”, el objeto de estudio de la ciencia jurídica se contrae a solo el ordenamiento normativo.

Siguiendo el lineamiento del positivismo jurídico, la idea de una norma fundamental que valida el sistema legal en su totalidad podemos relacionarlo con la idea de que las leyes de protección de datos personales también tienen una base fundamental que garantiza su validez y aplicabilidad. Esta norma fundamental es la Constitución Nacional y el conjunto de derechos fundamentales que respaldan la protección de la privacidad y de los derechos de los individuos en la revolución tecnológica que atravesamos.

Es por ello que la investigación se llevara a cabo desde un enfoque positivista empírico, a los fines de comprobar la utilidad y eficacia de las normas jurídicas con las que contamos en Argentina para resolver la Hipótesis planteada y proponer mejoras que hagan frente a una problemática que crece rápidamente, como lo es perfilamiento digital y la recopilación ilimitada de datos biométricos.

IV. 1. Objetivos del Trabajo de Investigación.

A. Objetivos Generales.

La presente investigación tiene por objetivo analizar y demostrar la necesidad de actualizar la ley de datos personales en vista de los cambios tecnológicos y sociales que estamos viviendo, con el fin de fortalecer la protección y privacidad de los individuos en la era digital.

B. Objetivos Específicos.

- Analizar la normativa vigente en materia de datos personales y contrastar con el Nuevo Proyecto de Reforma de la Ley de Protección de Datos personales. Con el fin de evaluar si las mejoras son significativas y eficaces para abordar la problemática del Perfilamiento Digital
- A través de una encuesta realizada, demostrar que nivel de conocimiento tiene la gente en materia de perfilamiento digital, con la finalidad de saber de qué manera brindan sus datos en internet y poder identificar los puntos de partida para brindar soluciones.

IV. 2. Metodología

El método que se utilizará para la investigación en la presente obra será el método hipotético con un análisis de tipo cuantitativo y cualitativo a través del análisis de la normativa actual en materia de datos personales, jurisprudencia nacional, como así también se mencionaran los métodos utilizados para recopilar datos personales con Inteligencia Artificial.

Dicho análisis será realizado en el “**Capítulo VI – Investigación**”.

La investigación se llevará a cabo de la siguiente manera:

- Análisis sobre el nuevo Proyecto de Ley de Datos personales y normas complementarias.
- A los fines de evaluar socialmente que nivel de conocimiento tienen los individuos sobre el perfilamiento digital y que recaudos toman al momento de interactuar en Internet, he optado por elegir como técnica de investigación la realización de una encuesta mediante Google Forms, la que contiene 6 preguntas formuladas en idioma claro y sencillo, contestada por 89 personas mayores de edad, de manera anónima.
- Conclusión y resolución.

Lo investigado tendrá por objeto probar que aspectos hay que mejorar e introducir en el nuevo Proyecto de Reforma de Ley de Datos personales a fin de hacer frente a la problemática existente a causa del Perfilamiento digital.

El modelo de encuesta a aplicar será:

Cuestionario de 6 preguntas.

CAPÍTULO V –

MARCO TEÓRICO ESPECÍFICO

El marco específico de la presente investigación se conforma por las normas existentes en nuestro país que son de aplicación en materia de protección de datos personales y que en la actualidad por analogía podrían aplicarse ante una problemática de perfilamiento digital, ya que hoy día no tenemos una ley que brinde soluciones específicas para hacer frente a dicha problemática.

1).- Marco normativo:

1. **Art. 43 Constitución Nacional:** Reforma de 1994. Siempre que no exista otro medio judicial más idóneo, dicho artículo otorga jerarquía constitucional a la acción de amparo, habeas corpus y habeas data, asimismo establece quienes poseen legitimación para interponerlo.

2. **Ley N° 25.326 Protección de Datos Personales (LPDP):** Creada en el año 2000. Tiene por objeto la protección de los datos personales asentados en medios de tratamientos de datos (archivos, bases de datos, etc), públicos o privados.

Otorga una definición a los conceptos: 1) Datos personales. 2) Datos sensibles.

3) Archivo, registro, base o banco de datos, indistintamente. 4) Tratamiento de datos. 5) Responsable de archivo, registro, base o banco de datos. 6) Datos informatizados. 7) Titular de los datos. 8) Usuario de datos. 9) Disociación de datos.-

Asimismo establece el marco legal en el que se deben recolectar los datos, la calidad de los mismos, el consentimiento que debe de existir por parte del titular de los datos ya que de lo contrario sería un tratamiento de datos personales ilícito, pues así lo determina esta ley, que también regula las obligaciones, medidas técnicas y prohibiciones, sanciones administrativas y sanciones penales que le caben en caso de incumplimiento al responsable del tratamiento de datos, sean entidades públicas o privadas.

3. **Decreto 1558/2001:** Crea la autoridad de aplicación que en su momento fue la Dirección Nacional de Protección de Datos, luego fue reemplazada por la Agencia de Acceso a la Información Pública.

4. **Decreto 1160/2010:** Modifica el inc. 3 del artículo 31 correspondiente al Anexo I del Decreto N° 1558/01 el cual trata sobre el proceso para la aplicación de sanciones.

5. **Ley 27.275 Derecho de Acceso a la Información Pública:** Sancionada en el año 2016 se creó con el objetivo de garantizar el ejercicio del derecho de acceso a la información pública y promueve la participación ciudadana y la transparencia de la gestión pública. Asimismo, creó la Agencia de acceso a la información pública (AAIP), desde ese momento autoridad de aplicación de la LPDP.

6. **Convenio 108:** Argentina adhirió en el año 2017 al Convenio 108 del Consejo de Europa respecto del Tratamiento Automatizado de Datos de Carácter Personal que se llevó a cabo en año 1981 en la ciudad de Estrasburgo. Este instrumento multilateral tiene por objeto proteger la privacidad de los individuos contra posibles abusos en el tratamiento de sus datos.

7. **Resolución AAIP E4 /2018:** Aprueba mejoras para las prácticas de la Ley 27.275.

8. **Resolución AAIP 5 /2018:** Establece como procedimiento interno de la AAIP,

la intervención obligatoria de la Dirección Nacional de Datos personales, en los reclamos por incumplimiento previstos en la ley N° 27.275 que afecten o puedan afectar la protección de datos personales. Tiene por finalidad que la DNDP emita un informe respecto a cada caso particular, para ser agregado al expediente electrónico que se genera.

9. **Resolución AAIP 40 /2018:** Aprueba un Modelo de Política de Protección de Datos

Personales para Organismos Públicos y recomienda a aquellos organismos públicos que sean titulares de bases de datos personales la adopción de la misma o similar, así como su difusión hacia la ciudadanía.

10. **Resolución AAIP 47/2018:** Aprueba medidas de seguridad relacionadas con el tratamiento y la conservación de datos personales en medios informatizados.

11. **Resolución AAIP 48/2018:** Da pautas para la determinación y el entendimiento del interés público, con la finalidad de elucidar controversias entre el interés público y la vigencia de otros derechos, así como facilitar el trámite de acceso a la información.

12. **Resolución AAIP 132/2018:** Establece que las inscripciones, modificaciones o bajas de bases de datos de datos personales ya sean de carácter público o privado deberán tramitarse exclusivamente a través de la plataforma TAD o GDE.

13. **Resolución AAIP 4/2019:** En su Anexo I define criterios orientadores e indicadores de mejores prácticas en la aplicación de la Ley N° 25.326.

Criterio 1. Derecho de acceso a datos personales recolectados mediante sistemas de video vigilancia; Criterio 2. Tratamiento automatizado de datos; Criterio 3. Disociación de datos; Criterio 4. Datos biométricos; Criterio 5. Consentimiento.

14. **Resolución 119/2022:** Creación del expediente administrativo conforme lo dispuesto por el Art. 12 del Decreto N° 1172/03 mediante el cual se invita a sectores interesados y a la ciudadanía en general en la elaboración de normas administrativas y de proyectos de ley para ser elevados por el Poder Ejecutivo Nacional al Honorable Congreso de la Nación, la resolución apunta a toda persona física o jurídica, pública o privada, que invoque un derecho o interés simple, difuso o de incidencia colectiva, para que en el plazo de QUINCE (15) días hábiles a partir de la publicación de la misma, presente sus propuestas y opiniones sobre la propuesta de Anteproyecto de Ley de Protección de Datos Personales.

15. **Resolución AAIP N°145/22:** Prorroga el plazo de la consulta pública sobre la propuesta del anteproyecto de la LPDP Res. 119/22, la misma se inició el 12 de Septiembre hasta el 30 de Septiembre y se prorrogó con la presente Resolución hasta el 11 de Octubre de 2022. *A lo largo del proceso se recibieron CIENTO SETENTA Y TRES (173) opiniones, aportes y comentarios presentados por CIENTO VEINTITRÉS (123) participantes representantes de la ciudadanía en general, organizaciones de la sociedad civil, universidades e investigadores, del sector privado y del sector público nacional e internacional.*⁷

16. **Ley N° 27.699:** Promulgada y publicada en el B.O en Noviembre del 2022, la misma aprueba el PROTOCOLO MODIFICATORIO DEL CONVENIO PARA LA PROTECCIÓN DE LAS PERSONAS CON RESPECTO AL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONAL, también conocido como Convenio 108+. Las modificaciones más destacadas del Convenio 108+:

- Se reconocen nuevos derechos para los titulares de datos
- Se actualizan los mecanismos de transferencias internacionales.

⁷ AAIP (Junio 2023). Mensaje 87/2023 “Proyecto de Ley de Protección de Datos Personales” [Archivo PDF] https://www.argentina.gob.ar/sites/default/files/mensajeyproyecto_leydpd2023.pdf. Consultado: 09/08/2023

- Se amplía el concepto de datos sensibles, pasando a incluir datos genéticos y biométricos.
- Se obliga a informar incidentes de seguridad.
- Se incorporan requisitos más estrictos respecto a los principios generales sobre tratamiento de datos, como el principio de proporcionalidad, de minimización de datos y licitud.
- Se Incluye condiciones especiales para el tratamiento de datos personales de niños y niñas.
- Se refuerza la exigencia de la destrucción y/o anonimato de datos personales.

2.- Nuevo Proyecto de Ley de Protección de Datos Personales.

Luego de la consulta pública abierta mediante Res. AAIP 119/22 y AAIP 145/22 y de recolectar las opiniones e investigaciones de distintos sectores de la sociedad, las cuales fueron analizadas y adoptadas por la AAIP, el 30 de Junio del 2023 el Poder Ejecutivo envió a la Congreso de la Nación el mensaje 87/2023 con el Proyecto de Ley de Protección de Datos Personales, cuyo propósito es modificar el régimen actual sancionado hace más de 20 años con la Ley 25.326.

El proyecto sigue los lineamientos del Reglamento General de Protección de Datos de la Unión Europea (“RGPD”)⁸ entre otros tratados internacionales

Las principales modificaciones:

Se modifica el Art. 2° agregando y actualizando las definiciones, se incorporan datos biométricos y datos genéticos:

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.

⁸ REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 [Archivo PDF] <https://www.boe.es/doue/2016/119/L00001-00088.pdf>. Consultado: 09/08/2023

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 para su obtención, recolección, formación, almacenamiento, organización o acceso.

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

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

Datos informatizados o nube de computación: Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado, incluyendo el contenido en aquel modelo en cual un tercero brinda infraestructura, plataformas o servicios de software para habilitar acceso conveniente por demanda a un conjunto compartido de recursos computacionales configurables, por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios, que pueden ser rápidamente aprovisionados y liberados con un esfuerzo mínimo de administración o de interacción con el proveedor de servicios.

Datos Biométricos: Datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona humana que permitan o confirmen su identificación única.

Datos Genéticos: Datos personales relativos a las características genéticas heredadas o adquiridas de una persona humana que proporcionen una información sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.

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.

Responsable del tratamiento: Toda persona física o persona de existencia ideal, pública o privada, titular de la base de datos, que decide sobre el tratamiento de datos, sus finalidades y medios.

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

Ámbito de aplicación material y territorial.

Se incorpora el concepto de extraterritorialidad, dentro del ámbito de aplicación, es decir que la ley se aplicara aun en los casos en que los responsables del tratamiento no se encuentran en el país.

Principios

Se establecen los principios que servirán como base de todo tratamiento de datos personales:

Principio de neutralidad: Sera de aplicación de la ley y sus reglamentaciones en cualquier tratamiento de datos personales con independencia de las técnicas, procesos o tecnologías en que fuera llevado a cabo el tratamiento actual o futuro.

Principio de licitud, lealtad y transparencia: El tratamiento de datos será lícito siempre que sea llevado a cabo en el marco de lo que indica la ley, asimismo indica que será un tratamiento leal y transparente si el Responsable lo hace absteniéndose de utilizar medios engañosos y si la información utilizada es fácilmente accesible, con un lenguaje sencillo y claro, respectivamente.

Principio de finalidad: Los datos deben ser recolectados con fines legítimos, explícitos y legítimos. Es compatible con ello los fines estadísticos, de archivo, de investigación científica o interés público.

Principio de minimización: Los datos deben ser tratados con la finalidad para los que fueron recolectados y a solicitud de la autoridad los Responsables deberán justificar la necesidad de tratar los datos.

Principio de exactitud: Los datos deben ser veraces, comprobables y actualizados. En caso de que sea necesaria su actualización, se deben adoptar las medidas necesarias para que no se altere la veracidad de los mismos. En el caso que los datos sean proporcionados por su Titular, se presume su exactitud.

Principio de preeminencia: En caso de duda, prevalecerá la ley más favorable para el Titular.

Plazo de conservación: Los datos no deben ser mantenidos más allá del tiempo que sea necesario para el cumplimiento del tratamiento. Podrán conservarse durante más tiempo cuando la finalidad sea científica o de interés público.

Principio de responsabilidad proactiva y demostrada: El o los Responsables podrán adoptar las medidas que consideren necesarias a fin de garantizar el cumplimiento de las obligaciones para el tratamiento lícito de datos personales.

Consentimiento y revocación

Se establecen las bases legales en las que podrá llevarse a cabo el tratamiento, entre ellas que el Titular brinde su consentimiento, y que podrá revocar el mismo en cualquier momento y sin fundamentación. La revocación debe de ser ofrecida por el responsable del tratamiento de datos de manera sencilla y gratuita.

Información al titular de los datos

El responsable del tratamiento debe brindar la información estipulada en el proyecto de manera accesible, concisa y bien explicada para el titular de los datos.

Tratamiento de datos sensibles

Se prohíbe el tratamiento de datos sensibles, a excepción de los siguientes supuestos:

a) El Titular de los datos ha dado su consentimiento a dicho tratamiento, salvo en los casos en que por ley no sea requerido el otorgamiento de dicha autorización;

b) Fuera necesario para salvaguardar el interés vital del Titular de los datos y éste se encontrará física o legalmente incapacitado para prestar el consentimiento y sus representantes legales no pudieran realizar en tiempo oportuno;

c) Es efectuado por establecimientos sanitarios públicos o privados o por

Profesionales vinculados a la ciencia de la salud con la finalidad de un tratamiento médico específico de acuerdo a lo establecido por la ley N° 26.529 de Derechos del Paciente, Historia Clínica y Consentimiento Informado y sus modificatorias: se prohíbe a los operadores de planes privados de salud tratar datos de salud para la práctica de selección de riesgo en la contratación de cualquier modalidad y la exclusión de

Beneficiarios;

d) Se realiza en el marco de las actividades legítimas de una fundación, asociación o cualquier otro organismo sin fines de lucro, cuyo objeto principal sea una actividad política, filosófica, religiosa o sindical. Siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan un contacto regular por razón de su objeto

principal, y que los datos personales no se comuniquen fuera de ellos sin el Consentimiento de los Titulares;

e) Se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;

f) Tuviera una finalidad histórica, de archivo de interés público, de aporte al proceso de memoria, verdad y justicia frente a crímenes de lesa humanidad, estadística o científica; en estos casos y en la medida de lo posible, debe adoptarse, teniendo en cuenta la finalidad, un procedimiento de anonimización o seudonimización;

g) Fuera necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del Responsable del tratamiento o del Titular de los datos en el ámbito del derecho laboral y de la seguridad, la salud pública y la protección social;

h) Sea necesario en ejercicio de las funciones de los poderes del Estado en el cumplimiento estricto de sus competencias. Cuando los organismos públicos traten datos personales sensibles, deben proveer condiciones más estrictas de seguridad, lo que debe implementarse mediante salvaguardas apropiadas adicionales, diseñadas específicamente.

i) Se realiza en el marco de la asistencia humanitaria.

Se estipula el especial tratamiento de datos sensibles, debiendo implementarse mayor seguridad confidencialidad y restricciones de uso.

Tratamiento de datos del sector público:

Para el sector público incluyendo Fuerzas Armadas, de seguridad y de inteligencia, rigen las mismas obligaciones que las estipuladas en el art. 13 para los Responsables. Cuando se trata de una cesión de datos personales, al Responsable a quien se ceden queda sujeto a las mismas obligaciones que el Responsable cedente.

Tratamiento de datos de niñas, niños y adolescentes:

Cuando se traten datos personales de menores de edad o adolescentes siempre se debe privilegiar la protección del interés superior del niño y los derechos consagrados en la CONVENCIÓN SOBRE LOS DERECHOS DEL NIÑO, aprobada por Ley N° 23.849 y demás instrumentos internacionales de los que la Nación es parte.

Es válido el consentimiento de menor o adolescente cuando se aplica al tratamiento de datos vinculados a la utilización de servicios de la sociedad de la información específicamente diseñados o aptos para ellos

Sera valido cuando el menor alcance los TRECE (13) años, en caso de ser menor de esa edad podrá dar su consentimiento informado o podrá ser otorgado por el Titular de la responsabilidad parental o quien se encuentre a cargo del niño/a

Sera obligación del Responsable adoptar las medidas necesarias a fin de verificar que el consentimiento fue otorgado por el adulto a cargo.

Se prohíbe el tratamiento de datos vinculado a juegos, aplicaciones o innovaciones tecnológicas que involucren información personal no vinculada con lo estrictamente relacionado con la finalidad de la actividad.

Es responsabilidad del Estado y de las instituciones educativas proporcionar información y brindar capacitación a los menores de edad y adolescentes acerca de los posibles riesgos relacionados con el manejo inadecuado de sus datos personales recae en el Estado y en las instituciones educativas, como así también informar sobre su derecho a la privacidad, la autodeterminación informativa y el respeto a los derechos de los demás.

Principio de seguridad de los datos personales y notificación de incidentes

Se establece las medidas de seguridad que debe adoptar el responsable de los datos personales a los fines de evitar y minimizar cualquier pérdida o utilización indebida ya sea por intención humana o por el medio tecnológico utilizado. Se fija como plazo 48 hs para la notificación de cualquier incidente de seguridad que constituya un riesgo para los derechos de los Titulares de los datos.

Deber de confidencialidad

El o los responsables del tratamiento de los datos están obligados a la confidencialidad respecto de los datos personales. Esta obligación subsiste aun después de finalizada su relación con el Titular de los datos.

Transferencias Internacionales

Al igual que en la LPDP en esta sección comprendida por los art. 22 a 26 se autoriza la transferencia de datos personales siempre que el país u organismo proporcione un nivel de protección adecuado.

Según la AAIP se considera que existe un nivel de protección adecuado cuando *“Se entiende que un Estado u organismo internacional proporciona un nivel adecuado de protección cuando dicha tutela se deriva directamente del ordenamiento jurídico vigente, o de sistemas de autorregulación.”*⁹

Asimismo, refiere a transferencias que deben ajustarse a una decisión de adecuación; mecanismos que permitan ofrecer las garantías adecuadas o excepciones,

⁹ AAIP- Obligaciones de los responsables de bases de datos personales <https://www.argentina.gob.ar/aaip/datospersonales/responsables/obligaciones> Consultado 26/08/2023.

que deben darse bajo ciertas condiciones y no pueden utilizarse de manera periódica o habitual.

Se establecen las siguientes excepciones siempre que se encuentren sujetas derechos humanos aplicables a la materia:

- a) Que el Titular de los datos haya otorgado su consentimiento;
- b) Que la transferencia sea necesaria para la ejecución de un contrato entre el Titular de los datos y el Responsable del tratamiento, o en beneficio del Titular de los datos, entre el Responsable de tratamiento y otra persona humana o jurídica, o para la ejecución de medidas precontractuales adoptadas a solicitud del Titular de los datos;
- c) Que la transferencia sea necesaria:
 - (I) Por razones de interés público;
 - (II) Para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;
 - (III) Para proteger los intereses vitales del Titular de los datos o de otras personas, si estuviera física o jurídicamente incapacitado para otorgar su consentimiento.

Derecho de los titulares de los datos

El capítulo IV del proyecto, comprendido por los art. 27 y 35 regula los derechos de los Titulares:

- a) Derecho de acceso: Previa identificación, el Titular tiene derecho a solicitar información sobre sus datos personales, en ningún caso se puede brindar información sobre terceros aunque estén relacionadas con el Titular.
- b) Derecho de rectificación: El Titular tiene derecho a solicitarle al Responsable la rectificación de sus datos personales en el caso de que sean inexactos, erróneos, etc. El Responsable debe cumplir con lo solicitado y rectificar o eliminar lo que no corresponda, según el caso.
- c) Derecho de oposición: Si no ha prestado consentimiento, el Titular puede oponerse al tratamiento de sus datos personales.

En el caso de que el tratamiento de datos personales sea con fines de interés público, patrimonio del Estado, investigación científica, o si los mismos son necesarios para esclarecer casos graves (violación de derechos humanos, crímenes de guerra o lesa humanidad) no procede la supresión.

- d) Decisiones automatizadas y elaboración de perfiles: Se entiende como decisión automatizada en las que no hay intervención humana significativa.

El Titular tiene derecho a no ser objeto de una decisión automatizada, se incluye en este caso a la elaboración de perfiles, tiene derecho a solicitar la revisión de los mismos por una persona humana, expresar su punto de vista e impugnar la decisión.

e) Derecho a la portabilidad de datos personales: El Titular tiene derecho a obtener una copia de los datos personales que hubiere proporcionado, salvo excepciones en las que no procede si se encuentran afectados terceros o los intereses y derechos del Responsable.

f) Derecho de limitación: el Titular tiene derecho de limitación en los casos que:

- El Titular impugne en tiempo prudencial que permita al Responsable verificar la información;
- Es un tratamiento ilícito y se solicita la limitación de su uso
- El Responsable conserva pero ya no necesita los datos para el fin del tratamiento y el interesado los necesita para el ejercicio o la defensa de sus derechos.
- En los casos estipulados en el Art. 29¹⁰ (derecho de oposición).

Todo individuo que haya obtenido una limitación, debe ser notificado por el Responsable antes del levantamiento de dicha medida.

En caso de que el Titular se vea en la necesidad de recurrir ante la autoridad competente por mediar una negativa por parte del Responsable, la limitación se extiende hasta la resolución del procedimiento por parte de la autoridad.

Ejercicio de los derechos y excepciones

Los derechos del titular de los datos son irrenunciables, el Responsable del tratamiento debe cumplir con los derechos del Titular dentro de los diez días hábiles de haber sido notificado fehacientemente. Los derechos y las garantías que otorga el proyecto de ley podrán ser limitadas por la autoridad competente siempre en pos de salvaguardar el interés y la seguridad pública.

El Titular queda habilitado a instar la acción judicial correspondiente por daños y perjuicios en caso de incumplimiento.

¹⁰ **ARTÍCULO 29.** - *Derecho de oposición. El Titular puede oponerse al tratamiento de sus datos o de una finalidad específica de éste, si no ha prestado consentimiento. El Responsable del tratamiento debe dejar de tratar los datos personales objeto de oposición, salvo que existan motivos legítimos para el tratamiento que prevalezcan sobre los derechos del Titular de los datos. El Titular también puede oponerse al tratamiento de sus datos personales si tuvieran por objeto la publicidad, la prospección comercial o la mercadotecnia directa, incluida la elaboración de perfiles, en la medida que esté relacionada con esas finalidades. Cuando el Titular se oponga al tratamiento para esos propósitos, sus datos personales deben dejar de ser tratados para dichos fines. El Titular tiene derecho a que el tratamiento de datos personales se limite a su almacenamiento durante el período que medie entre una solicitud de rectificación u oposición hasta su resolución por el Responsable. (AAIP- Proyecto de Ley de Protección de Datos Personales - Febrero 2023.*

Obligaciones de los responsables y encargados del tratamiento

En esta sección comprendida por los art. 34 a 46 se establecen los deberes del Responsable y del Encargado del tratamiento, como así también las medidas para el cumplimiento de las obligaciones, se crea también la figura del Delegado quien será designado por los Responsables o Encargados.

Para el caso de un grupo de empresas, tienen la opción de designar a un solo delegado de protección de datos. Esta función puede ser desempeñada por un trabajador del Responsable o bajo un acuerdo de prestación de servicios.,

Los Responsables del tratamiento deben: cumplir con la obligación de implementar medidas necesarias y tendientes a demostrar el adecuado cumplimiento de la normativa.

Los datos deben ser reales y actualizados, garantizándole al Titular la supresión o rectificación en caso de corresponder.

Deben tratar los mismos bajo condiciones de seguridad que minimicen los riesgos de adulteración, pérdida o uso no autorizado.

Deben tramitar y responder en el plazo legal establecido las consultas realizadas por el Titular.

Debe existir un instrumento jurídico adecuado que estipule la prestación de servicios entre el Responsable y el Encargado.

El Responsable debe verificar previo a designar al Encargado que ofrezca la garantía suficiente para estar a cargo del tratamiento de datos personales y así garantizar los derechos del Titular.

En caso de corresponder, se deberá designar un Delegado de Protección de datos, o una persona o área que asuma ese rol.

Los Encargados del tratamiento deben:

- La relación entre el Responsable y el Encargado deberá quedar formalizada mediante un contrato o instrumento jurídico acorde.

- El Encargado solo podrá llevar a cabo el tratamiento indicado por el Responsable.

- Los datos personales que sean objeto del tratamiento no podrán ser utilizados para otro fin, ni cedidos, salvo expresa autorización del Responsable.

- Finalizada la relación contractual, los datos personales deben ser devueltos al Responsable o destruidos, si razonablemente se puede presumir que a futuro existirá nuevamente una relación contractual, estos datos pueden conservarse por DOS AÑOS.

- Permitir al Responsable o Autoridad la auditoria o inspección con el fin de controlar el cumplimiento de lo estipulado en el contrato y en la ley.
- El Encargado podrá subcontratar servicios para ejercer el tratamiento de datos personales solamente si se encuentra autorizado por el Responsable. Asumiendo el rol del Responsable en caso de incumplimiento por parte del subcontratado.
- Deben informar en el plazo legal estipulado cualquier incidente de seguridad al Responsable y a la Autoridad.

Tanto los Responsables como los Encargados deben diseñar políticas a los fines de asegurar la seguridad en el tratamiento de datos personales, brindándole al Titular un lenguaje claro y sencillo.

En los casos en que el Responsable planea llevar a cabo el tratamiento de datos que por su naturaleza o alcance es probable que implique un riesgo o afectación a los derechos de los Titulares, deberá realizar una evaluación de impacto, la misma deberá contener los requisitos establecidos en el Art. 42.¹¹

En caso de que el resultado sea positivo y efectivamente el tratamiento implique un riesgo o afectación, se deberá realizar un informe previo a la Autoridad con los requisitos estipulados en el Art. 43¹².

Delegado de protección de datos: Se incorpora esta figura que deberá ser designada por los Responsables y Encargados, en los supuestos que se trate de una autoridad u organismo público o si las actividades del Responsable o del Encargado necesitaren un control permanente.

¹¹ **ARTÍCULO 42.** - Contenido de la evaluación de impacto. La evaluación debe incluir, como mínimo: a. Una descripción sistemática de las operaciones de tratamiento de datos previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el Responsable del tratamiento; b. Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento de datos con respecto a su finalidad; c. Una evaluación de los riesgos para la protección de los datos personales de los Titulares a que se refiere el inciso a) del artículo 41; d. Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de los datos personales, y para demostrar la conformidad con la presente ley, teniendo en cuenta los derechos e intereses legítimos de los Titulares de los datos y de otras personas que pudieran verse potencialmente afectadas. (AAIP- Proyecto de Ley de Protección de Datos Personales - Febrero 2023. Fecha de consulta: 25/08/2023)

¹² **ARTÍCULO 43.** - Informe previo. Cuando una evaluación de impacto muestra que el tratamiento entrañará un alto riesgo, el Responsable debe informar de esta circunstancia a la Autoridad de aplicación. El informe debe incluir, como mínimo: a. Las obligaciones respectivas del Responsable y Encargado, en particular en caso de tratamiento de datos dentro de un mismo Grupo económico; b. Los fines y medios del tratamiento previsto; 31c. Las medidas y garantías establecidas para minimizar los riesgos identificados y proteger los derechos de los Titulares; d. En su caso, los datos de contacto del Delegado de protección de datos; e. La evaluación de impacto relativa a la protección de datos; f. Cualquier otra información que solicite la Autoridad de aplicación. El Responsable no podrá iniciar el tratamiento de datos hasta tanto la Autoridad de aplicación se pronuncie sobre el informe. (AAIP- Proyecto de Ley de Protección de Datos Personales - Febrero 2023.

La designación debe recaer en una persona que resulte idónea y con los conocimientos necesarios para llevar a cabo la función.

El Responsable o Encargado se encuentra obligado a respaldar y brindarle la información y herramientas necesarias al Delegado para su desempeño.

El Delegado solo debe responder ante el nivel jerárquico más alto de la organización.

Protección de información crediticia y derecho al olvido

Se regula la protección de datos de información crediticia y se establece como plazo de conservación de los mismos en las bases de datos CINCO años desde la última información significativa y UN año si el deudor cancele o extinga la obligación.

Ámbito de aplicación

Se establece a la AAIP como autoridad de aplicación y sus facultades.

Procedimientos y sanciones

En caso de constatarse algún incumplimiento a la ley, se establecen nuevos criterios para la fijación de las multas sujetos al Índice de Precios al Consumidor, que vale destacar, desde el año 2000 no se actualizaba.

Además, se estipula que la Autoridad podrá iniciar procedimientos en los casos que:

- Sea el Titular quien inste el procedimiento ante la Autoridad.
- Sea la Autoridad de aplicación quien inicie el procedimiento
- Sea un tercero, organización o asociación que tenga algún interés legítimo

y que efectuó la denuncia por violación de la ley.

El reclamo es gratuito y primeramente se debe intimar al Responsable, pasados los 30 días desde que se efectuó la comunicación, mediando respuesta o no del Titular, el interesado podrá iniciar la presentación ante la Autoridad, quien intimara al Responsable o Encargado por el plazo de 15 días a que manifieste lo que estime corresponder y ofrezca las pruebas que considere necesarias.

Una vez cumplido, la Autoridad evaluara las infracciones si las hubo y labrara un acta de la cual se dará traslado mediante notificación al Responsable, quien tendrá el derecho a efectuar su descargo por el plazo de 5 días.

En el caso de que la acción sea instada por la Autoridad o por un tercero, organización o asociación con un interés legítimo, será de aplicación la ley Nacional de Procedimientos Administrativos N° 19.549¹³.

En el caso de que la acción sea instada por el Titular, la Ley 19.549 será de aplicación supletoria.

La Autoridad mediante resolución podrá:

- Desestimar las denuncias.
- Hacer lugar a la denuncia e intimar al Responsable o Encargado por el plazo de 15 días a que dé cumplimiento con los derechos de protección estipulados por ley.
- En caso de incumplimiento, imponer sanciones.

Una vez notificada la resolución, el interesado podrá interponer dentro de los 15 días el recurso de reconsideración correspondiente.

Para este trámite no procede el recurso de Apelación.

La resolución efectuada por la Autoridad agota la vida administrativa.

Para el caso de instar la acción judicial corresponde hacerlo ante el fuero Federal o Contencioso Administrativo.

Acción de Habeas Data

De manera similar a la LPDP vigente, se regula especialmente la acción judicial de habeas data, la innovación aquí la encontramos en la legitimación activa en reclamos por acción colectiva.

La finalidad del Hábeas Data es que el particular damnificado pueda tomar conocimiento de los datos que tienen que ver con su persona y cuál es la finalidad de los mismos, lo que le permitirá posteriormente ante peticionar ante el Juez correspondiente, la rectificación, actualización, supresión, de los datos.

Legitimación activa y pasiva:

Poseen legitimación activa para obrar el Titular, el responsable a cargo del menor o en el caso de personas fallecidas por sus sucesores universales y procede contra Responsables o Encargados, quienes al mismo tiempo y en caso de corresponder excepcionalmente podrán interponer la acción contra otros Responsables o Encargados.

Competencia:

¹³ Ley 19.549 (27/4/1972)– <https://servicios.infoleg.gob.ar/infolegInternet/anexos/20000-24999/22363/texact.htm> . Consultado 27/08/2023

La competencia se establece por el domicilio del actor o del demandado, a elección de quien inste la acción.

Cuando el reclamo se trate del sector Público la competencia que corresponde es el fuero Federal.

Admisibilidad y procedimiento:

El procedimiento de Habeas Data se llevara a cabo mediante lo estipulado en el presente proyecto de reforma similar al establecido en la Ley 25.356, y supletoriamente según corresponda tramitara bajo las normas del amparo común y procesalmente en lo que respecta al juicio sumarísimo.

Para la admisibilidad de la demanda se establece que deberá interponerse por escrito y contener la mayor precisión posible en la individualización de los datos.

Es importante destacar que la garantía constitucional de Habeas Data tutela derechos tan fundamentales como la privacidad, la imagen, la autodeterminación informativa, el honor.

Es por ello que el Titular deberá identificar las razones por las cuales entiende que el tratamiento de datos que se está efectuando es indebido y los motivos que le asisten para interponer el reclamo.

Si es manifiesto que los datos son inexactos o falsos, el juez como medida provisoria podría ordenar el bloqueo de los mismos.

Admitida la acción el Juez requerirá al archivo, registro o banco de datos la remisión de la información concerniente al accionante. Podrá asimismo solicitar informes sobre el soporte técnico de datos, documentación de base relativa a la recolección y cualquier otro aspecto que resulte conducente a la resolución de la causa que estime procedente.

El plazo para contestar lo solicitado no podrá ser mayor de cinco días hábiles, aunque podrá ser ampliado en caso de corresponder, por el Juez.

Al contestar, no se podrá alegar la confidencialidad de la información que se les requiere salvo el caso en que se afecten las fuentes de información periodística, asimismo y el archivo, registro o banco de datos deberá explicar las razones por las cuales incluyó la información cuestionada y aquellas por las que no evacuó el pedido efectuado por el interesado.

Sentencia

Una vez vencido el plazo para contestar, se haga uso de este derecho o no y produciéndose la prueba en caso de corresponder, el Juez dictara sentencia y en su caso especificara que decisión ha tomado respecto de la información, si ha de suprimirse, actualizarse, rectificarse, estableciendo un plazo para su cumplimiento.

En caso de ser rechazada la acción in limine, por no cumplir con los requisitos para la admisibilidad de la demanda, la resolución no producirá efecto de cosa juzgada.

En caso de rechazo de la acción, no constituye presunción respecto de la responsabilidad en que hubiera podido incurrir el demandante.

3.- PERFILAMIENTO DIGITAL

El denominado Perfilamiento Digital, resulta ser en la actualidad una de las problemáticas más preocupante que trae consigo el tratamiento de datos , ya que las técnicas utilizadas son cada vez más invasivas, recopilando información sobre la personalidad, sus preferencias, características, orientación política, sexual, religiosa y demás información sensible con la que se va creando un perfil digital de la persona, que luego puede ser consultado por entidades públicas o privadas según la finalidad.

La regulación en la materia es poca y la sociedad no cuenta con la información necesaria, muchas veces se brindan datos sin tener acceso a toda la información ya que por lo general es confusa y no se muestra de manera sencilla para los usuarios, como, por ejemplo, los permisos que solicitan las aplicaciones, las opiniones que damos en redes sociales, las fotos que subimos, las ubicaciones que compartimos, toda esa información que brindamos voluntariamente es recolectada y analizada, creando de nosotros un perfil digital, sin nuestro consentimiento y muchas veces el mismo puede contener errores o vulneraciones a nuestros derechos personalísimos.

Un evento muy reciente que ha sucedido en nuestro país relacionado con los datos personales ha sido en Agosto del 2023, con la llegada de Worldcoin, una empresa creada por Sam Altman (uno de los creadores de OpenAI), la misma realizo una campaña en distintos puntos del país, ofreciendo alrededor de 50 dólares estadounidenses a cambio de que las personas accedan a vender sus datos biométricos mediante un scan del iris con la ayuda de The Orb un lector digital que escanea la biometría del iris en segundos.

Lo cierto es que, en el contexto actual del país, en el mes de las elecciones, la suba del dólar, hizo que miles de ciudadanos accedieran a vender sus datos biométricos sin conocer los peligros de tal práctica.

Fueron tantas personas que el caso tomo relevancia y la AAIP inició una investigación contra Worldcoin, solicitando datos para verificar que la empresa está tomando todas las medidas a su alcance para proteger la privacidad de los ciudadanos que participan en el proyecto.

Según explicó la AAIP, la Fundación Wordcoin debe seguir los procedimientos establecidos en la Ley de Protección de Datos Personales, que incluyen registrarse en la institución, entregar información sobre sus políticas de tratamiento de datos, indicar el motivo por el que se requieren los datos e informar sobre el tiempo de conservación de esta información.

Además, Worldcoin también debe detallar las medidas de seguridad y confidencialidad que aplica para salvaguardar la información personal de los ciudadanos argentinos.¹⁴

Anteriormente en el año 2021, el ReNaPer ha detectado que mediante el uso de claves otorgadas al Ministerio de Salud, se han filtrado fotos, domicilios, e información relacionada a figuras públicas, lo que llevo a crear una Política de mejoras mediante Disposición N° 1/2022, la innovación de dicha disposición es que en cuanto a eventuales “incidentes de seguridad”, se dispone la obligación de comunicarlos a la Dirección Nacional de Ciberseguridad y a la AAIP en un plazo no superior a las 48 hs. de haber tomado conocimiento, junto con las medidas correctivas y paliativas implementadas y/o a implementar por el Organismo para minimizar las consecuencias.

4.- ¿Qué son los datos biométricos?

Los sistemas de reconocimiento biométrico son: «un sistema de reconocimiento de personas por uno o más rasgos físicos o de comportamiento (a través de una foto tridimensional de la cara y/o cuerpo, una muestra de voz, las huellas dactilares, la localización de las venas de la mano, el tipo de sangre, una foto de la córnea del ojo, etc.)»¹⁵

Tanto el sistema público como privado utiliza la recolección de datos biométricos para distintos fines.

¹⁴ Worldcoin: Argentina abrió una investigación sobre sus actividades y el tratamiento de los datos que obtiene (10 de Agosto de 2023) <https://tn.com.ar/tecn/novedades/2023/08/10/worldcoin-argentina-abrio-una-investigacion-sobre-sus-actividades-y-el-tratamiento-de-los-datos-que-obtiene/>
Consultado:17/08/2023

¹⁵ RIVERA, Julio C., en «Derecho a la intimidad», La Ley, 1980-D, 912

En el sector privado se utilizan, por ejemplo, como método de control en el ámbito laboral, comparto el pensamiento del Dr. Lanzavechia *“La situación del otorgamiento de los registros biométricos importa una desacertada práctica, desde óptica protectoria del trabajador, puesto que se encuentra entregando - involuntariamente - una porción de su vida privada; que puede incluso ser utilizada a futuro, vaya a saber para qué, bajo un otorgamiento de consentimiento limitado.”*¹⁶

En el sector público, un ejemplo es el ANSES con el sistema conocido como Mi Huella, según la página oficial: *“Es un sistema que permite reconocer la identidad de las personas a través de la digitalización de las huellas dactilares para facilitar la realización de trámite.”*¹⁷

Lo cierto es que también está estrictamente vinculado con el sector privado ya que intervienen en la relación entidades financieras y bancarias, a los fines de brindar seguridad jurídica la resolución 648/2014 señala que los datos biométricos recolectados por ANSES serán resguardados en una única Base de Datos de Registros Biométricos que será administrada por la Dirección General Diseño de Normas y Procesos.

Otro ejemplo del sector público es el ReNaPer, un ente con jurisdicción Nacional, dependiente del Ministerio del Interior, entre sus funciones estipuladas en la Ley 17.761 tiene por objeto *“La clasificación y procesamiento de la información relacionada con la persona”*

Es decir, que fue creado con el objeto de administrar los datos de todas las personas humanas del territorio Argentino y para garantizar la preservación, custodia y tratamiento lícito de la información personal se encuentra alcanzado por la ley 25.326 LPDP y Ley 17.671.

Lo mismo sucede con AFIP, que registra los datos biométricos faciales, y de comportamiento de los individuos.

Ahora bien, podemos concluir que si bien la LPDP se encuentra desactualizada, los organismos Estatales encargados de recolectar datos biométricos para el cumplimiento de sus servicios se encuentran obligados a brindar un marco de

¹⁶ Lanzavechia, Gabriel E. -LA INTELIGENCIA ARTIFICIAL EN EL EJERCICIO DE LA FACULTAD DE CONTROL EN EL ÁMBITO LABORAL Y EL RESERVORIO DE DATOS BIOMÉTRICOS DE LOS TRABAJADORES: ¿AFECTACIÓN A LOS DERECHOS PERSONALÍSIMOS? Fecha: 03-09-2021. Cita: MJ-DOC-16144-AR | MJ16144

¹⁷ ANSES, Registro de Mi Huella. <https://www.anses.gob.ar/jubilaciones-y-pensiones/consultas-y-tramites-frecuentes-para-jubilados/registro-de-mi-huella#:~:text=Mi%20Huella%20es%20un%20sistema,no%20necesit%C3%A1s%20enrolar%20tu%20huella.> Consultado: 22/08/2023

seguridad jurídica y custodia de los mismos y que en caso de que haya un incumplimiento o uso indebido de los mismos, el Titular de los datos tiene el derecho a solicitar información o iniciar la acción judicial correspondiente.

Un problema mayor surge cuando el propio usuario en la inmensidad de la Internet es quien brinda sus datos personales o biométricos en Sitios Webs o Aplicaciones desconociendo el peligro que eso supone y en consecuencia son utilizados indebidamente o la persona termina siendo víctima de algún ciberdelito, como es el “*phishing*” una técnica utilizada para robar datos personales y contraseñas, otro escenario mas que demuestra la necesidad imperiosa de educar a la sociedad y reformar las leyes en miras de proteger los datos personales que se han vuelto valiosos para empresas como estrategias de marketing

5.- Fallos Nacionales

B) “P. A. E. c. Facebook Argentina SRL s/ medida autosatisfactiva”¹⁸:

En la provincia de Mendoza, el actor se presenta ante la justicia a los fines de proteger los derechos de sus hijos menores de edad, interpone una medida autosatisfactiva contra Facebook Argentina SRL, solicitando se eliminen publicaciones que contenían el nombre de sus hijos como así también imágenes y solicita se ordene a determinados perfiles a abstenerse de usar enlaces o cualquier otro espacio que vulnere o afecte de cualquier manera el nombre, honor, imagen, intimidad, o integridad de sus hijos.

El Juez de grado admitió y otorgo la medida, que fue apelada por la demandada, quien invoco la falta de legitimación pasiva argumentando que no se encuentra habilitada a operar el sitio web www.Facebook.com, por cuanto las condiciones aceptadas por los usuarios no son ante Facebook Argentina sino Facebook Inc.

El Tribunal Superior confirmó el pronunciamiento del Juzgado de origen en cuanto a la improcedencia de la excepción de falta de legitimación pasiva. En efecto, el tribunal entiende que aun cuando el procesamiento de los datos es realizado por una entidad extranjera (Facebook Inc.), la conexión existente con la filial local, constituida bajo la ley argentina y sometida a ella, que realiza una

actividad comercial vinculada con el servicio de la primera, deriva en la aplicación de la norma local. La Cámara sostuvo que “*Facebook, más allá de la estructura*

¹⁸ Medida autosatisfactiva. Derecho a la imagen. Menores de edad. Publicaciones indebidas. Legitimación pasiva de Facebook Argentina SRL (Mayo 2019) <http://e-procesal.com/medida-autosatisfactiva-derecho-a-la-imagen-menores-de-edad-publicaciones-indebidas-legitimacion-pasiva-de-facebook-argentina-srl-2097>
Consultado: 16/08/2023

de representación y formas sociales adoptadas por la empresa para cada país, se encuentra constituida comercialmente en nuestra República como Facebook Argentina SRL, quedando, en consecuencia, sometida a la legislación argentina.”

C) “Giolito c. Google Argentina SRL y Google LLC”¹⁹

Se inicia la causa con una denuncia interpuesta ante la AAIP por la actora M.C.G contra GOOGLE ARGENTINA SRL en relación con el ejercicio de su derecho de acceso, consagrado en el artículo 14 de la Ley N° 25.326.

La denunciante reclama que un tercero no autorizado ingreso a su cuenta de Gmail, modificándole sus datos de ingreso y eliminando el acceso de todos los dispositivos, en consecuencia, se produjo la pérdida de información valiosa.

Primeramente, reclamo ante GOOGLE ARGENTINA SRL mediante misiva en la que solicita la restitución inmediata de toda su información, la que no fue satisfecha ya que GOOGLE ARGENTINA SRL alego que rechazaba la misma por improcedente y que *“Google Argentina SRL no administra ni tiene responsabilidades técnicas sobre Gmail, producto administrado por Google LLC”, aclarando que Google LLC es una sociedad cuyo domicilio está en el extranjero, razón por la cual allí se “deberá dirigir cualquier reclamo relacionado con dicho servicio”.*

A raíz de la denuncia ante la AAIP por intermedio de la Dirección Nacional de Protección de Datos Personales se intimo en el plazo de 10 días hábiles a GOOGLE ARGENTINA SRL a que le permitan ejercer a la denunciante el acceso a sus datos, conforme a la definición de dato personal prevista en el Art. 2 de la Ley N° 25.326 y al derecho contenido en el Art. 14 de la misma Ley.

Como respuesta a lo solicitado GOOGLE ARGENTINA SRL opuso una suerte de falta de legitimación pasiva ya que declaró que *“no administra ni tiene responsabilidades técnicas sobre el servicio de correo electrónico Gmail” y que el servicio es administrado exclusivamente por GOOGLE LLC. También sostuvo que no representa a GOOGLE LLC, que no presta servicios en Internet ni colabora con GOOGLE LLC en la administración de Gmail*”. Asimismo, argumento que *“Considera que sólo los tribunales judiciales son competentes para dar trámite a la acción de protección de datos. Ello así de conformidad con el artículo 36 de la Ley N° 25.326, que prevé que “será competente para entender en esta acción el juez del domicilio del actor; el del domicilio del demandado; el*

¹⁹ Resolución Giolito c. Google Argentina SRL y Google LLC - EX-2019-84609512- -APNDNPDP#AAIP. 13 de Abril de 2020 [Archivo PDF] https://www.argentina.gob.ar/sites/default/files/rs-2020-25457045-apn-aaip_google.pdf Consultado: 16/08/2023

del lugar en el que el hecho o acto se exteriorice o pudiera tener efecto, a elección del actor”.

La Dirección Nacional mediante la NO-2019-102933822-APN-DNPDP#AAIP, realizó un análisis de los argumentos vertidos por GOOGLE ARGENTINA SRL, concluyendo que la AAIP tiene competencia para entender sobre los reclamos de los titulares de datos bajo la Ley N° 25.326 y que GOOGLE LLC no solo debe responder no solo debe responder ante los estrados judiciales, sino ante dicha autoridad administrativa.

Por último, la autoridad local consideró que Google Argentina, que opera como agente comercial de la matriz, es una representación de Google LLC para todas las notificaciones y comunicaciones que fueran necesarias.

A raíz de ello, la AAIP inició la instrucción de sumario. Las demandadas nuevamente alegaron lo ya manifestado y cuestionaron las facultades de la autoridad para solicitar la entrega de la información que se solicita.

Planteos que fueron rechazados y en consecuencia como las empresas no han dado cumplimiento a sus obligaciones impuestas por la LPDP y aplicó la sanción de pesos 180.000 a Google Argentina y pesos 100.000 a Google LLC por no otorgar el derecho de acceso al titular del dato y, a su vez, por no haber colaborado con la AAIP, respectivamente.

6.- Derecho Comparado

Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108) – UE:

El fin del Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona («protección de datos»).

Reglamento General de Protección de Datos – UE (RGPD):

El Reglamento es una herramienta esencial en la actual era digital, que facilita la actividad económica, ya que aclara las normas aplicables a las empresas y los organismos públicos en el mercado único digital. Además, unifica la normativa, para los distintos sistemas nacionales y pone fin a las cargas administrativas innecesarias.

Dio origen al Comité Europeo de Protección de Datos (CEPD).

Estándares de protección de datos personales de la red Iberoamericana de Protección de Datos (RIPD):

Conjunto de principios y derechos de protección de datos personales para que los Estados Iberoamericanos puedan adoptar y desarrollar en su legislación nacional, con la finalidad de garantizar un debido tratamiento de los datos personales y contar con reglas homogéneas en la región.

Principios actualizados sobre la privacidad y la Protección de Datos Personales – OEA:

Establece 13 Principios que reflejan las distintas aproximaciones que prevalecen en los Estados miembros sobre los temas centrales de la protección de los datos personales, entre ellos el consentimiento, las finalidades y medios para la captación y tratamiento de estos datos, el flujo transfronterizo y la seguridad de los datos personales, la protección especial a los datos sensibles, y el ejercicio de los derechos de acceso, rectificación, cancelación, oposición y portabilidad.

Recomendación sobre la Ética de la Inteligencia Artificial – UNESCO: Primer instrumento normativo mundial sobre el tema. No solo protegerá, sino que también promoverá los derechos humanos y la dignidad humana, y será una brújula guía ética y una base normativa global que permitirá construir un sólido respeto por el estado de derecho en el mundo digital.

Ley General de Protección de Datos (LGPD) – Brasil.

Ley Orgánica de Protección de Datos Personales - Ecuador.

CAPÍTULO VI - INVESTIGACIÓN

Para llevar a cabo la investigación de manera efectiva, resulta necesario hacer una breve referencia sobre los métodos más comunes, reconocidos y empleados para el procesamiento de datos personales. Esto permitirá posteriormente contrastar los datos obtenidos a través de la encuesta realizada por quien suscribe, mediante Google Forms acerca del perfilamiento digital y el uso de datos biométricos.

1.-ANÁLISIS E INTERPRETACION DE LOS RESULTADOS:

Introduccion:

Como método de investigación, he realizado una encuesta sobre Perfilamiento Digital y Datos Biométricos mediante Google Forms, los resultados a la encuesta realizada serán analizados mediante porcentajes estadísticos para apreciar de una manera correcta la información obtenida.

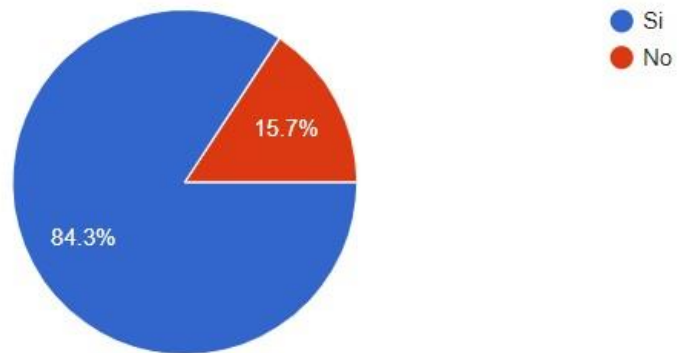
Cabe destacar que participaron de la misma 89 personas mayores de edad en el rango etario de 20 a 60 años, de manera anónima, con preguntas relacionadas a las decisiones de la vida cotidiana en la utilización de redes sociales.

Luego de haber analizado los datos recopilados en la encuesta mencionada, se presentan a continuación los resultados obtenidos:

Primera pregunta.

1.- ¿Sabías que existe una Ley de Protección de Datos Personales?

89 respuestas



Como luce en el grafico acompañado, del 100% de las personas encuestadas, un 84,3% (75 personas) tienen conocimiento de la existencia de una Ley de Protección de Datos Personales y el 15,7% (14 personas) no sabían de su existencia.

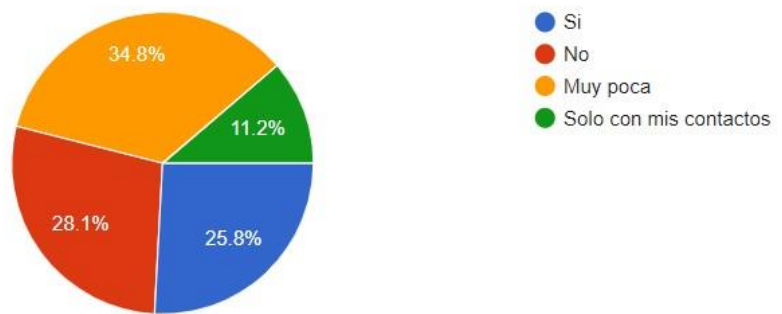
Es un resultado alentador y demuestra que a pesar de ser una ley que existe hace 23 sugiere que una parte significativa de los encuestados se encuentra informada sobre sus derechos en lo que respecta al manejo de sus datos personales y las obligaciones de las entidades que los tratan. El nivel de conocimiento sobre protección de datos personales en la sociedad es esencial para promover prácticas adecuadas de recopilación, almacenamiento y uso de datos personales.

Sin embargo, los 14 encuestados que declararon no tener conocimiento sobre la ley de datos personales representan una minoría que podría beneficiarse de una mayor divulgación de información y educación sobre este tema. Esto sugiere que todavía existe margen para mejorar la educación en la materia y asegurarse de que todos los ciudadanos estén informados sobre sus derechos y responsabilidades en relación con sus datos personales.

Segunda pregunta

2.- ¿Compartís tus datos personales en redes sociales?

89 respuestas



Conforme a los resultados obtenidos, se refleja que la mayoría de los encuestados, esto es exactamente un 34,8% (31 personas) comparten “Muy pocos” datos personales en sus redes sociales, lo que da indicios de que un segmento considerable de los participantes es consciente de los riesgos asociados con la divulgación de datos personales en las redes sociales. Esto sugiere una actitud más cautelosa y un grado de responsabilidad hacia la importancia de limitar la cantidad de información compartida en plataformas públicas.

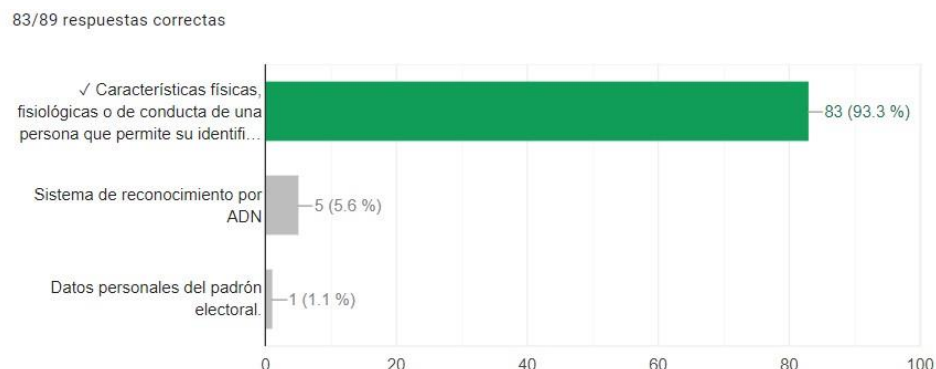
Siguiendo los resultados, el 28,1% (25 personas) de los encuestados que respondió "No" muestra una proporción importante de individuos que eligen protegerse de compartir datos personales en redes sociales. Esto puede indicar la presencia de una preocupación social significativa por la privacidad y la seguridad de la información personal que se brinda en Internet.

Por su parte, el 25,8% (23 personas) que respondió "Sí" indica que aún existe un grupo relevante de personas dispuestas a compartir sus datos personales en redes sociales. Puede deberse a distintas razones, existe mundialmente la comodidad frente a la exposición en redes sociales sin evaluar los peligros, como también puede deberse a una falta de información o educación en materia de datos personales.

El 11,2% (10 personas) que contestó "Solo con mis contactos" refleja un intento en la búsqueda de restringir la audiencia sobre la información compartida, un esfuerzo por mantener un mayor control sobre quiénes pueden acceder a los datos personales, sin embargo no es una conducta que garantice la protección de datos personales.

Tercera pregunta.

3.- ¿Que son y para qué sirven los datos biométricos?



Favorablemente la mayoría de los encuestados 93,3% (83 personas) tienen conocimiento sobre la definición y utilidad de los datos biométricos. Lo cual representa un escenario alentador.

La alta proporción de respuestas correctas sugiere que existe un nivel razonable de conocimiento, lo cual es crucial en un mundo cada vez más digital y centrado en la tecnología. La información sobre los datos biométricos es esencial para una toma de decisiones informada con el fin de proteger la privacidad y la seguridad en contextos que involucran la recopilación y el uso de características físicas única, lo cual se puede dar en un marco laboral o en relaciones de consumo.

Sin perjuicio de ello, el pequeño porcentaje de respuestas incorrectas nos muestra la necesidad de continuar educando a la sociedad.

Cabe reiterar que solo participaron de la encuesta personas mayores de edad, en el caso de los menores de edad según una encuesta realizada en 2018 por la Defensoría del Pueblo en escuelas públicas y privadas de la Ciudad Autónoma de Buenos Aires, los alumnos tenían un celular propio desde los nueve (18,9%) y diez años (30,7%), y comenzaban a usar las redes sociales a los diez años (33,4%)²⁰. Esto refleja que por la corta edad y el esperable desconocimiento en el tema, junto con la difícil tarea de control sobre los dispositivos, son el sector de la población que más expuesto se encuentra y que más protección necesita.

²⁰ Defensoría del Pueblo. SEGUNDA ENCUESTA SOBRE PROTECCIÓN DE DATOS PERSONALES Y USO DE DISPOSITIVOS MÓVILES E INTERNET EN NIÑOS Y NIÑAS EN EDAD ESCOLAR (Mayo de 2016) https://defensoria.org.ar/archivo_noticias/segunda-encuesta-sobre-proteccion-de-datos-personales-y-uso-de-dispositivos-moviles-e-internet-en-ninos-y-ninas-en-edad-escolar/ Consultado: 26/08/2023.

Respecto de las personas mayores según un estudio realizado en 2022 por la Defensoría del Pueblo denominado “Personas mayores y el uso de la tecnología” ²¹el mismo reflejo en cuanto a la utilidad que le dan a los dispositivos móviles, el 88,6% declaró para buscar información de su interés, el 88,3% que lo hace para comunicarse con otros, el 82,3% para hacer trámites o pedir turnos médicos, el 60,5% ve películas y/o vídeos (estas últimas dos se duplicaron en comparación a la pre pandemia). Mientras que el 71,2% lo ha incorporado para educarse y un 60% para realizar operaciones bancarias y pagos de impuestos.

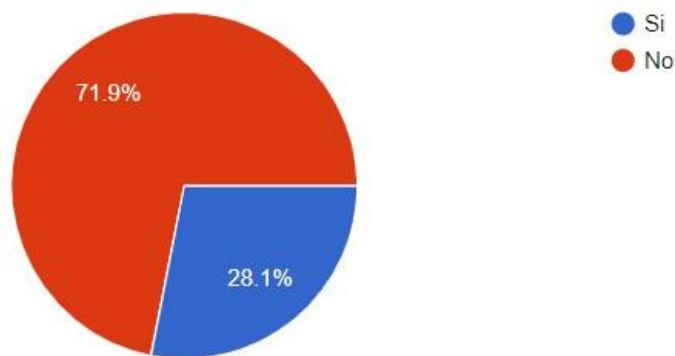
Al consultarlos si tienen reparos a la hora de usar las tecnologías de la información y la comunicación (TIC), el 61.1% respondió que NO y el 88,6% indicó que cuida mucho o bastante su privacidad.

Si bien estos resultados son alentadores en relación a la comodidad que presentan las personas mayores con el uso de la tecnología, el desafío se encuentra en garantizar el uso consciente y efectivo de los dispositivos para la protección de los datos personales.

Cuarta pregunta.

4.- ¿Lees los términos y condiciones en Internet antes de aceptarlos?

89 respuestas



Los resultados obtenidos a esta pregunta en donde el 71,9 % (64 personas) admiten NO leer los términos y condiciones antes de aceptarlos y el 28,1 (25 personas) SI, este escenario puede reflejar una falta de conciencia y de educación respecto a los

²¹ Defensoría del Pueblo. PERSONAS MAYORES Y EL USO DE LA TECNOLOGÍA: LA PROTECCIÓN PERSONAL DE NUESTROS DATOS (Junio del 2022) <https://defensoria.org.ar/entradas-cdpd/personas-mayores-y-el-uso-de-la-tecnologia-la-proteccion-personal-de-nuestros-datos/> Consultado: 26/08/2023.

datos personales, sin embargo, en contraste con las respuestas anteriores, otro motivo podría ser la falta de lenguaje claro y lo dificultoso que resulta leerlos y entenderlos para el usuario.

Los términos y condiciones generalmente están redactados en un lenguaje legal complejo que puede ser difícil de entender para el público en general. Esto puede dificultar la comprensión de los usuarios y llevar a la aceptación sin un entendimiento verdadero.

Según la definición del Ministerio de Justicia y Derechos Humanos: *“Son las cláusulas legales que establecen la forma en la que puedes usar la información y acceder a los contenidos de una página web o de una aplicación. También establecen lo que el dueño de la página o aplicación hará con tus datos personales y con los datos que generes cuando uses las aplicaciones o servicios. Son condiciones unilaterales. Tenés que aceptarlas para poder usar los servicios de la página web. Cuando aceptás los términos y condiciones das tu consentimiento para que la empresa almacene, procese, analice o utilice tus datos para distintos fines.”*²²

Siguiendo ese lineamiento, la aceptación de los Términos y condiciones sin tomar conocimiento de los mismos, tiene consecuencias negativas en la protección de datos personales, ya que estos pueden incluir detalles importantes sobre cómo se recopilan, utilizan y comparten los datos del usuario. La falta de lectura puede llevar a una aceptación indiscriminada de cláusulas que podrían limitar los derechos de privacidad y el control sobre los propios datos. Los Titulares pueden estar renunciando a ciertos derechos sin darse cuenta, lo que potencialmente debilita su capacidad de tomar decisiones informadas sobre el manejo de sus datos.

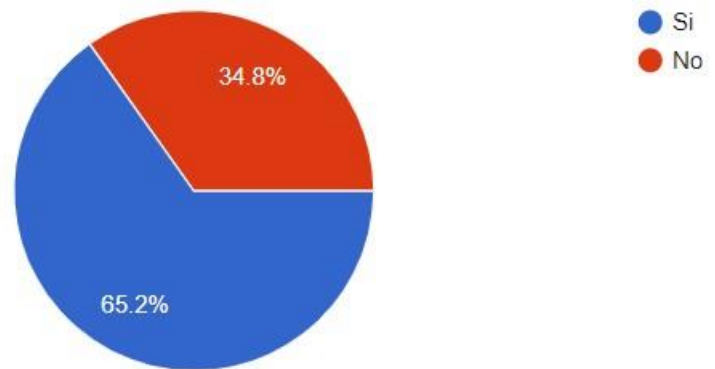
Las respuestas obtenidas reflejan uno de los principales motivos por los cuales existe una desprotección de datos personales y la necesidad de implementar el lenguaje claro y accesible que propone el Nuevo Proyecto de Reforma de la LPDP.

Quinta pregunta.

5.- ¿Configuras los permisos que tienen las aplicaciones para acceder a tu cámara, galería de fotos y/o micrófono?

²² Ministerio de Justicia y Derechos Humanos. ¿Por qué es importante leer los términos y condiciones de una página en internet o aplicación? (Junio de 2023) <https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/porque-es-importante-leer-los-terminos-y-condiciones-de-una-pagina-en-internet-o-aplicacion> Consultado: 27/08/2023.

89 respuestas



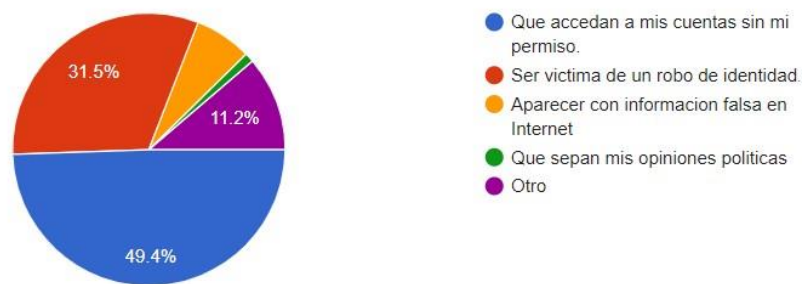
El grafico acompañado supra demuestra que el 65,2% (58 personas) tienen conocimiento de los peligros que implica brindar permiso ilimitado a las aplicaciones. Configurar adecuadamente los permisos ayuda a prevenir el uso indebido de la cámara, galería de fotos y micrófono, lo que potencialmente evita la exposición de información sensible y la grabación no autorizada.

Si bien es positivo el número de encuestados que si se manejan de manera responsable a los fines de proteger sus datos personales, lo cierto es que el 34,8% (31 personas) que NO configura la privacidad y los permisos que otorgan a las aplicaciones es un número importante de individuos que se encuentran expuestos a sufrir el uso no deseado de sus datos.

Sexta pregunta

6.- ¿Qué es lo que más te preocupa sobre tu privacidad en Internet?

89 respuestas



Para finalizar la encuesta y a los fines de tomar dimensión sobre las preocupaciones de los encuestados al utilizar Internet, la mayoría ha mostrado preocupación a sufrir un acceso no permitido a sus cuentas, esto es el 49,4% (44 personas). El acceso no autorizado puede exponer información personal, como datos personales, conversaciones privadas, fotos y archivos, a terceros con fines ilícitos.

Al 31,5% (28 personas) le preocupa ser víctima de un robo de identidad, este delito se conoce también como “*Phishing*”, según la Secretaria de Innovación Publica se define como “*El robo de identidad o phishing es la obtención de información sensible de alguien a fin de extraer dinero de sus cuentas, o de sus allegados, o bien suplantar la identidad digital/cuentas de la víctima. Una persona puede también hacerse pasar por una organización, como un banco o servicio de una empresa u organismo público, solicitando cargar datos bancarios en una página que simula pertenecer a la entidad.*”²³

Al 6,7% (6 personas) le preocupa “Aparecer con información falsa en Internet”, esta respuesta se encuentra estrictamente ligada con el perfilamiento digital, aunque cabe recordar que el perfilamiento digital no se limita solo a la información falsa. La recopilación de datos en línea también puede conducir a la creación de perfiles precisos que se utilizan para orientar anuncios y contenido, lo que puede ser beneficioso para personalizar experiencias en línea. Sin embargo, también puede resultar violatorio en términos de privacidad y consentimiento informado.

La respuesta de las 10 personas que mencionaron esta preocupación sugiere que un grupo muy reducido de personas del total de encuestados, son conscientes de los posibles riesgos del perfilamiento digital.

Por último el 11,2% (10 personas) contestaron “Otro” y 1,1% (1 persona) contesto que su preocupación es que sepan sus opiniones políticas.

²³ Ciberseguridad. Datos personales: Phishing o robo de identidad
<https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/recomendaciones-de-3> Consultado: 27/08/2023.

CAPÍTULO VII –

CONCLUSIÓN.

La investigación ha logrado a través de la implementación de una encuesta que se conformó por 89 participantes, mayores de edad, corroborar la hipótesis inicial de que es necesario una regulación normativa más estricta en el ámbito del tratamiento de datos personales, incluyendo datos biométricos y mayor información para los titulares de datos, con el fin de proporcionar un marco sólido de seguridad jurídica que garantice el adecuado tratamiento y almacenamiento de datos.

Los resultados obtenidos en la encuesta proporcionan evidencia sólida en apoyo a la hipótesis planteada. La mayoría de los participantes han expresado tener un leve conocimiento en materia de datos personales y una preocupación a que ellos sean vulnerados por distintos motivos como es el ingreso no autorizado o falsificación de identidad.

Esta inquietud refleja una creciente conciencia sobre la importancia de proteger los datos personales, sin embargo no es suficiente para hacer frente al problema inminente sobre tratamiento indebido de datos, perfilamiento digital y recolección de datos biométricos.

La relación que hay entre las preocupaciones manifestadas por los encuestados y las protecciones legales que brinda la normativa actual denota la urgencia de una revisión y actualización de la LPDP como así también el papel que tiene el Estado frente a esta problemática.

En virtud de las pruebas recopiladas, queda demostrado que la hipótesis planteada es válida y respaldada por los datos obtenidos de la encuesta. La actualización de la ley de datos personales y la necesidad de que el Estado se involucre se presenta como una necesidad inminente en un entorno digital en constante cambio, donde la privacidad y la seguridad de los individuos se encuentran en constante peligro.

CAPÍTULO VIII –

PROPUESTA.

La protección de los datos personales es una preocupación creciente en la era digital. Para abordar la problemática del perfilamiento digital, es esencial que el Estado implemente una campaña de concienciación y educación dirigida a informar a la población sobre los riesgos y las mejores prácticas en este ámbito. Esta campaña podría llevarse a cabo a través de campañas publicitarias en medios masivos, como televisión, radio y medios en línea, para llegar a un público amplio. Organizar talleres y charlas educativas en comunidades, escuelas, universidades y espacios públicos para explicar en detalle los conceptos, riesgos y medidas de seguridad recomendadas en relación a la protección de datos personales.

Otra iniciativa a modo educativo podría ser incorporar leyendas o mensajes de privacidad en productos y aplicaciones, recordando a los usuarios la importancia de revisar la configuración de privacidad.

Además de la reforma de la LPDP, la creación de una ley específica en biometría que tenga por objeto definir las limitaciones y el alcance a la recopilación de datos biométricos por cualquier medio de recolección y en cualquier ámbito ya sea laboral, entidades financieras, social mediante aplicaciones, estableciendo una reglamentación para el almacenamiento y conservación y estipulando sanciones y multas en caso de incumplimiento, así también mejorar la tecnología a los fines de que las bases de almacenamiento sean mas seguras para hacer frente a cualquier ciberdelito.

Si bien el Nuevo Proyecto de reforma de la LPDP prevé la actualización de las multas, considero que para disuadir de manera efectiva el tratamiento ilícito de datos personales, es crucial implementar sanciones y multas más severas que actúen como un verdadero incentivo para el cumplimiento de las regulaciones de privacidad. Como así también obligar a que las organizaciones públicas y privadas brinden capacitación a su personal sobre la normativa de protección de datos.

BIBLIOGRAFÍA.

1.- GUIA DE BUENAS PRACTICAS EN PRIVACIDAD PARA EL DESARROLLO DE APLICACIONES - *Dirección Nacional de Protección de Datos Personales* (Microjuris Cita: MJ-LEG-70425-90001-AR||LEG70425)

2.- Lanzavechia, Gabriel E. -*LA INTELIGENCIA ARTIFICIAL EN EL EJERCICIO DE LA FACULTAD DE CONTROL EN EL ÁMBITO LABORAL Y EL RESERVORIO DE DATOS BIOMÉTRICOS DE LOS TRABAJADORES: ¿AFECTACIÓN A LOS DERECHOS PERSONALÍSIMOS?* Fecha: 03-09-2021. Cita: MJ-DOC-16144-AR||MJD16144

3.- MASCIOTRA, Mario: *Naturaleza jurídica del hábeas data argentino, 2004, en www.saij.jus.gov.ar, Id SAIJ: DACF040047.*

4.- RIVERA, Julio C., en «*Derecho a la intimidad*», *La Ley*, 1980-D, 912

5.- SAGUES, Néstor, "*Amparo, hábeas data y hábeas corpus en la reforma constitucional*", *La Ley* del 7/10/94.

Leyes

Derecho argentino

- Constitución Argentina.
- Código Civil y Comercial.
- Ley 25.326 - PROTECCION DE LOS DATOS PERSONALES (30 de Octubre de 2000)
- Ley 27.699- PROTOCOLO MODIFICATORIO DEL CONVENIO PARA LA PROTECCIÓN DE LAS PERSONAS CON RESPECTO AL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONAL (30/11/2022)
- Ley 27.275 Derecho de Acceso a la Información Pública (14-sep-2016)
- Ley 17.761 LEY DE IDENTIFICACION, REGISTRO Y CLASIFICACION DEL POTENCIAL HUMANO NACIONAL (29 de febrero de 1968)
- Decreto 1558/2001
- Decreto 1160/2010
- Resolución AAIP E4 /2018
- Resolución AAIP 47/2018

- Resolución AAIP 4/2019
- Resolución AAIP 48/2018
- Resolución AAIP 132/2018
- Resolución 119/2022
- Resolución AAIP N°145/22
- Resolución 648/2014 ANSES

Derecho comparado

- Ley N° 25.326 de Protección de Datos Personales.
- Antecedente 2018 - Proyecto de Ley de Protección de Datos Personales (perdió estado parlamentario).
 - Ley N° 27.483 de aprobación del Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.
 - Reglamento General de Protección de Datos (RGPD) - Unión Europea.
 - Estándares de Protección de Datos Personales de la Red Iberoamericana de Protección de Datos (RIPD).
 - Principios actualizados sobre la privacidad y la protección de datos personales, con anotaciones de la OEA.
 - Recomendación sobre la Ética de la Inteligencia Artificial - UNESCO.
 - Ley General de Protección de Datos (LGPD) - Brasil.
 - Ley Orgánica de Protección de Datos Personales - Ecuador.

Tratados Internacionales

- Convenio 108, suscrito en 1981 en la ciudad de Estrasburgo (Francia).

Otras fuentes

- **Exención de Mi Huella. - ANSES**

<https://www.anses.gob.ar/jubilaciones-y-pensiones/consultas-y-tramites-frecuentes-para-jubilados/registro-de-mi-huella/exencion-de-mi-huella#:~:text=Mí%20Huella%20es%20un%20sistema,casos%20puede%20solicitarse%20la%20exenci%C3%B3n.> - Consultado: 04/05/2022

- **Datos Biométricos. ANSES**

https://servicioscf.afip.gob.ar/publico/abc/ABCpaso2.aspx?id_nivel1=2949&id_nivel2=313

8&p=Datos%20Biom%C3%A9tricos#:~:text=Los%20datos%20biom%C3%A9tricos%20de
ben%20registrarse,la%20comisi%C3%B3n%20de%20dichos%20fraudes. Consultado:
04/05/2022

- **Klever Aníbal Guamán. El positivismo y el positivismo jurídico.**
Universidad y Sociedad vol.12no.4/02-Ago-2020
http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202020000400265#B6
Consultado: 25/08/2023

- **AAIP (Junio 2023). Mensaje 87/2023 “Proyecto de Ley de Protección de Datos Personales” [Archivo PDF]**
https://www.argentina.gob.ar/sites/default/files/mensajeyproyecto_leydpdp2023.pdf.
Consultado: 09/08/2023

- **REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 [Archivo PDF]**
<https://www.boe.es/doue/2016/119/L00001-00088.pdf>. Consultado: 09/08/2023

- **AAIP- Obligaciones de los responsables de bases de datos personales**
<https://www.argentina.gob.ar/aaip/datospersonales/responsables/obligaciones> Consultado
26/08/2023.

- **Ley19.549-(27/4/1972)–**
<https://servicios.infoleg.gob.ar/infolegInternet/anexos/20000-24999/22363/texact.htm>.
Consultado 27/08/2023

- **Worldcoin: Argentina abrió una investigación sobre sus actividades y el tratamiento de los datos que obtiene (10 de Agosto de 2023)**
<https://tn.com.ar/tecno/novedades/2023/08/10/worldcoin-argentina-abrio-una-investigacion-sobre-sus-actividades-y-el-tratamiento-de-los-datos-que-obtiene/>
Consultado:17/08/2023

- **Qué es Big Data.** <https://www.argentina.gob.ar/jefatura/innovacion-publica/telecomunicaciones-y-conectividad/grupo-de-trabajo-de-servicios-de-6>
Consultado: 22/08/2023

- **ANSES, Registro de Mi Huella.** <https://www.anses.gob.ar/jubilaciones-y-pensiones/consultas-y-tramites-frecuentes-para-jubilados/registro-de-mi-huella#:~:text=Mí%20Huella%20es%20un%20sistema,no%20necesit%C3%A1s%20enrolar%20tu%20huella>. Consultado: 22/08/2023

○ **Defensoría del Pueblo. SEGUNDA ENCUESTA SOBRE PROTECCIÓN DE DATOS PERSONALES Y USO DE DISPOSITIVOS MÓVILES E INTERNET EN NIÑOS Y NIÑAS EN EDAD ESCOLAR (Mayo de 2016)**

https://defensoria.org.ar/archivo_noticias/segunda-encuesta-sobre-proteccion-de-datos-personales-y-uso-de-dispositivos-moviles-e-internet-en-ninos-y-ninas-en-edad-escolar/

Consultado: 26/08/2023.

○ **Defensoria del Pueblo. PERSONAS MAYORES Y EL USO DE LA TECNOLOGÍA: LA PROTECCIÓN PERSONAL DE NUESTROS DATOS (Junio del 2022)**

<https://defensoria.org.ar/entradas-cpdp/personas-mayores-y-el-uso-de-la-tecnologia-la-proteccion-personal-de-nuestros-datos/> Consultado: 26/08/2023.

○ **Ministerio de Justicia y Derechos Humanos. ¿Por qué es importante leer los términos y condiciones de una página en internet o aplicación? (Junio de 2023)**

<https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/porque-es-importante-leer-los-terminos-y-condiciones-de-una-pagina-en-internet-o-aplicacion>

Consultado: 27/08/2023.

○ **Ciberseguridad. Datos personales: Phishing o robo de identidad**

<https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/recomendaciones-de-3> Consultado: 27/08/2023.

○ **Medida autosatisfactiva. Derecho a la imagen. Menores de edad. Publicaciones indebidas. Legitimación pasiva de Facebook Argentina SRL (Mayo 2019)**

<http://e-procesal.com/medida-autosatisfactiva-derecho-a-la-imagen-menores-de-edad-publicaciones-indebidas-legitimacion-pasiva-de-facebook-argentina-srl-2097>

Consultado: 16/08/2023

○ **Resolución Giolito c. Google Argentina SRL y Google LLC - EX-2019-84609512- -APNDNPDP#AAIP. 13 de Abril de 2020 [Archivo PDF]**

https://www.argentina.gob.ar/sites/default/files/rs-2020-25457045-apn-aaip_google.pdf

Consultado: 16/08/2023

NOTA DE ELEVACIÓN DE TESIS

CABA, Buenos Aires, 27 de Agosto de 2023

**Sr. Decano de la Facultad de Derecho y Ciencias Políticas
de la Universidad Abierta Interamericana.**

Dr. Marcos Córdoba.

S_____ / _____ D

De mi mayor consideración:

Por la presente comunico por este medio que la alumna **SURIANO FLORENCIA BELEN**, ha confeccionado bajo mi supervisión el trabajo final que lleva el título: ***“Perfilamiento digital. El límite a la recopilación de datos biométricos”***

Creo que por la calidad disciplinar de su contenido merece ser defendido ante el Tribunal que se designe.-

No asumo responsabilidad penal y/o civil por la presente obra, toda vez que la producción integral de la misma resulta exclusiva propiedad intelectual de la tesista; siendo el carácter de las instrucciones realizadas por el Suscripto, opiniones meramente metodológicas y orientadoras del área de incumbencia del trabajo de investigación.-

Sin otro particular, saludo a Ud. Atte.

Firma:

Apellido y Nombre: Suriano Florencia Belen

Domicilio: Caracas 4867

E-mail: Florenciasuriano1993@gmail.com

Estado de situación

Suriano, Florencia Belen

ABOGACÍA

Legajo: A0960006218-J1 / Estado: (BR) - Baja Regular / Campus: 091 UAI - CENTRO / Año: 4° / Turno: Noche / Letra: E

Suriano, Florencia Belen (A0960006218-J1)

27/08/2023

CARACAS 4867, CABA, Capital Federal, Argentina, C.P.
1419
Teléfono: (CEL) 1165119460; (HOG) 45721813; (LAB)
45730205

Documento: DNI - 38010239
Nacido en: Argentina
Fecha de Nacimiento: 03/12/1993

(J1 04) ABOGACIA (Ingreso: 01/04/2015)
Título Secundario: BACHILLER MERCANTIL - Egresado
en: 2011
Estado del certificado del Título Secundario:
Entregado legalizado

ASIGNATURAS DEL INGRESO

Curso	Fecha	Descripción	Nota
Curso de Ingreso (2015)	18/02/2015	COMUNICACIÓN ORAL Y ESCRITA	7.00

INSCRIPCION EN MATERIAS PARA: 2023

Año	Materia	Descripción	Horas	Etapas	Campus	Comisión	% Asistencia
-----	---------	-------------	-------	--------	--------	----------	--------------

* La inscripción de estas materias están sujetas a la cursada de sus correlativas.
** La inscripción de estas materias están sujetas a la regularización de sus correlativas.
B La inscripción de estas materias están en estado de Baja.

INSCRIPCION EN EXÁMENES

Fecha	Tipo	Asignatura	Presidente	Acta
-------	------	------------	------------	------

MATERIAS RENDIDAS

Año	Materia	Descripción	Nota	Fecha	Homologación-Situación de la materia	Inst. Orig.	Campus	Libro	Folio
2	J104 13	DERECHO PENAL I	2.00	2016-08-04			096	24	55
2	J104 14	MEDIOS ALTERNATIVOS DE RESOLUCIÓN DE CONFLICTOS	8.00	2016-08-09			096	24	70
2	J104 15	INGLÉS I	2.00	2016-08-10			096	24	80
2	J104 12	DERECHO CONSTITUCIONAL II	5.00	2016-08-08			096	24	63
2	J104 11	OBLIGACIONES CIVILES Y COMERCIALES	5.00	2016-12-14			096	24	115
2	J104 16	DERECHO INTERNACIONAL PÚBLICO	7.00	2016-12-12			096	24	103
2	J104 20	SEMINARIO DE INTEGRACIÓN I	7.00	2016-12-13			096	24	111

5	J104 41	FILOSOFÍA DEL DERECHO	8.00	2019-07- 29	096	26	65
4	J104 36	EL DERECHO DEL TRABAJO Y LA SEGURIDAD SOCIAL	8.00	2019-08- 08	096	26	88
4	J104 30	DERECHOS REALES	6.00	2019-12- 09	096	26	96
5	J104 39	DERECHO DE FAMILIA	6.00	2019-12- 11	096	26	100
4	J104 32	DERECHO FINANCIERO Y TRIBUTARIO	8.00	2020-08- 06	091	89	50
5	J104 44	DERECHO SUCESORIO	8.00	2020-08- 03	091	88	181
1	J104 03	PROBLEMÁTICA DEL MUNDO ACTUAL	8.00	2020-07- 29	091	88	111
4	J104 34	DERECHO PROCESAL PENAL	7.00	2020-07- 31	095	40	23
5	J104 40	RECURSOS NATURALES Y MEDIO AMBIENTE	6.00	2020-08- 04	091	89	06
3	J104 27	DERECHO ADMINISTRATIVO II	8.00	2020-12- 14	091	89	169
5	J104 45	DERECHO INTERNACIONAL PRIVADO	7.00	2020-12- 10	095	40	92
5	J104 46	METODOLOGÍA DE LA INVESTIGACIÓN JURÍDICA	8.00	2020-12- 15	091	89	192
2	J104 15	INGLÉS I	7.00	2020-12- 09	091	89	97
2	J104 18	PSICOLOGÍA APLICADA AL DERECHO	10.00	2020-12- 16	091	90	07
2	J104 19	INGLÉS II	9.00	2021-03- 22	091	91	09
3	J104 25	INGLÉS III	7.00	2021-03- 22	091	91	10
5	J104 47	DERECHO DE LA INTEGRACIÓN	7.00	2021-03- 23	091	91	15
4	J104 35	CONCURSOS Y QUIEBRAS	8.00	2021-08- 05	091	91	100
4	J104 33	SOCIOLOGÍA DEL DERECHO	7.00	2021-12- 16	091	92	117
4	J104 --	ECONOMÍA POLÍTICA	8.00	2021-12- --	091	92	139

Año	Materia	Descripción	Nota	Fecha	Homologación-Situación de la materia	Inst. Orig.	Campus	Libro	Folio
4	J104 37	PRÁCTICA PROFESIONAL CIVIL Y COMERCIAL II	9.00	2021-12-21			091	93	03
1	J104 01	INTRODUCCIÓN AL DERECHO	8.00	2015-07-29			096	23	16
1	J104 02	DERECHO POLÍTICO	6.00	2015-08-04			096	23	49
1	J104 04	INTRODUCCIÓN AL PENSAMIENTO CIENTÍFICO	8.00	2015-07-27			096	23	04
1	J104 08	HISTORIA DE LAS INSTITUCIONES ARGENTINAS	7.00	2015-12-09			096	23	86
1	J104 09	DERECHO ROMANO	6.00	2015-12-10			096	23	102
1	J104 06	DERECHO CIVIL. PARTE GENERAL	8.00	2015-12-15			096	23	134
1	J104 07	DERECHO CONSTITUCIONAL I Y DERECHOS HUMANOS	5.00	2015-12-21			096	23	177
5	J118 28	INTERPRETACIÓN DEL DERECHO	9.00	2020-07-30	J104 49 Optativa		091	88	150
5	J104 73	DERECHO DEL DEPORTE	8.00	2020-08-06	J104 48 Optativa		090	40	122
5	J104 87	DERECHO DE LOS NEGOCIOS INTERNACIONALES	7.00	2021-12-22	J104 42 Optativa		091	93	28

Fecha de última materia: 22 de Diciembre de 2021
Promedio: 7.20833333333333 - No se consideran aplazos.
Promedio: 7 - Se consideran aplazos.

2	J104 20	SEMINARIO DE INTEGRACIÓN I	7.00	2016-12- 13		096	24	111
2	J104 13	DERECHO PENAL I	7.00	2016-12- 15		096	24	123
2	J104 17	DERECHO PENAL II	6.00	2016-12- 22		096	24	167
3	J104 22	DERECHO ADMINISTRATIVO I	8.00	2017-08- 04		096	25	42
3	J104 23	DERECHO COMERCIAL	8.00	2017-08- 07		096	25	45
3	J104 24	DERECHO PROCESAL. PARTE GENERAL	8.00	2017-08- 09		096	25	61
3	J104 26	DERECHO SOCIETARIO Y CARTULAR	8.00	2017-12- 18		096	25	107

Año	Materia	Descripción	Nota	Fecha	Homologación-Situación de la materia	Inst. Orig.	Campus	Libro	Folio
3	J104 28	PRÁCTICA PROFESIONAL CIVIL Y COMERCIAL I	9.00	2017-12- 20			096	25	116
3	J104 29	DERECHO PROCESAL CIVIL	7.00	2017-12- 15			096	25	98
3	J104 21	CONTRATOS CIVILES Y COMERCIALES	6.00	2017-12- 19			096	25	112
1	J104 05	TALLER DE INFORMÁTICA I	4.00	2019-03- 25			091	85	08
5	J104 43	PORTUGUÉS	7.00	2019-03- 25			091	85	10
1	J104 10	TALLER DE INFORMÁTICA II	4.00	2019-03- 26			091	85	16
5	J104 41	FILOSOFÍA DEL DERECHO	8.00	2019-07- 20			096	26	65