

Protección de datos personales: Aspectos, panorama actual y su implementación en las Universidades Nacionales

Sequeira, Martín Julián

UNLaM (sequemartin1999@gmail.com)

Resumen— Este trabajo explora las implicancias del derecho a la protección de datos personales desde su inclusión en la reforma constitucional de 1994 y la Ley 25.326 hasta la situación actual. Asimismo, se analizará la figura del Delegado de Protección de Datos Personales, que, aunque no esté implementado legislativamente, es reconocido por la Agencia de Acceso a la Información Pública y en diversos proyectos de reforma. Por otro lado, se evaluará la viabilidad de implementar esta figura en universidades nacionales, teniendo en cuenta la Ley de Educación Superior y la Resolución 40/2018.

Abstract— This paper explores the implications of the right to personal data protection from its inclusion in the 1994 constitutional reform and Law 25.326 to the present situation. It will also analyze the role of the Data Protection Officer, which, although not legislatively established, is recognized by the Agency for Access to Public Information and various reform projects. Additionally, the feasibility of implementing this role in national universities will be assessed, considering the Higher Education Law and Resolution 40/2018.

I. INTRODUCCIÓN:

El avance de las nuevas tecnologías de la información y la comunicación ha traído consigo una serie de desafíos significativos que las organizaciones deben enfrentar en términos de ciberseguridad y protección de datos. La expansión del uso de herramientas digitales y la creciente dependencia de bases de datos para gestionar actividades en diversos sectores han intensificado la necesidad de abordar de manera efectiva las nuevas formas de criminalidad informática y garantizar la seguridad de la información almacenada.

A medida que las tecnologías evolucionan, también lo hacen las tácticas de los ciberdelincuentes, quienes explotan vulnerabilidades en los sistemas de información para llevar a cabo ataques que pueden comprometer la integridad, confidencialidad y disponibilidad de los datos personales. Esta situación ha llevado a un aumento en la preocupación por la protección de datos personales, un aspecto crítico dado que gran parte de la información gestionada por las entidades públicas y privadas se clasifica como datos personales.

Las universidades, en particular, se enfrentan a desafíos únicos en este contexto. Estas instituciones no solo manejan grandes volúmenes de datos personales relacionados con el

alumnado, el personal docente y no docente, y las actividades de investigación, sino que también tienen la responsabilidad de garantizar la seguridad y privacidad de esta información. La naturaleza sensible de los datos que gestionan hace que la protección adecuada sea esencial para preservar la integridad de las operaciones académicas y administrativas.

Para abordar estos desafíos de manera efectiva, es crucial contextualizar tanto las normativas que regulan el funcionamiento de las universidades como el marco legal de protección de datos personales. Este análisis buscará propiciar una comprensión integral del derecho a la protección de datos personales. La protección de datos busca garantizar que la información personal sea gestionada de manera segura y respetuosa. Desde su incorporación en la Constitución Nacional en 1994, este derecho ha evolucionado, pasando de una visión centrada en la intimidad a una perspectiva más amplia que permite a los individuos controlar la información personal que sobre ellos se almacena y utiliza. En este contexto, la figura del Delegado de Protección de Datos Personales juega un papel crucial. Esta figura actúa como un nexo entre la autoridad de protección de datos y la organización, asegurando el cumplimiento de las regulaciones y políticas de privacidad. Además, entre otras tareas asesora sobre la correcta implementación de prácticas de protección de datos, supervisa los procedimientos internos, realiza auditorías y gestiona incidentes de seguridad relacionados con los datos personales.

Finalmente, es fundamental considerar el panorama actual y la implementación de estas prácticas en el ámbito universitario. Las universidades deben evaluar cómo integrar la figura del Delegado de Protección de Datos Personales en sus políticas de protección de datos. Aunque la legislación vigente en Argentina, no menciona explícitamente la figura del Delegado de Protección de Datos Personales, las resoluciones de la Agencia de Acceso a la Información Pública y los proyectos de reforma legislativa sugieren la incorporación de esta figura para asegurar una gestión adecuada de los datos personales.

A razón de lo expuesto es que en el presente trabajo se propone realizar un análisis de estos temas con el objetivo de compatibilizar el derecho a la protección de datos personales con la normativa que regula las universidades. Se examinará el alcance de las responsabilidades del Delegado de Protección de Datos Personales de datos personales y cómo estas pueden ser adaptadas al contexto universitario en Argentina.

* Revista Argentina de Trabajos Estudiantiles. Patrocinada por la IEEE.

II. PROTECCIÓN DE DATOS PERSONALES.

El derecho de protección de datos personales surge en nuestro ordenamiento jurídico con su incorporación en el artículo 43 de la Constitución Nacional en la reforma de 1994. La incorporación del instituto del amparo especial de protección de datos Personales o habeas data ampara desde su génesis el derecho a la Protección de datos Personales, la misma fue incorporada bajo el nombre de amparo especial, debido a la falta de habilitación expresa en la ley declarativa de reforma. Como menciona Oscar R. Puccinelli *para evitar impugnaciones constitucionales, se la guaresció bajo el molde de amparo, que era una de las figuras habilitadas para su incorporación en el artículo... pese a que su génesis se la vinculaba directamente con la otra figura habilitada, de la que tomó su nomen iuris: el habeas corpus*. [1]

Es importante mencionar que el alcance de la protección que brinda este instituto en principio estaba vinculado al derecho a la intimidad. Autores como el Dr. Quiroga Lavié han sostenido *que la reforma de 1994 incorporó en el artículo 43, párrafo 3° la acción de hábeas data que, en alguna de sus especies, funciona como medio de protección tanto de la intimidad como de la privacidad (remitimos al estudio especial del amparo como género de tutela dentro del subprincipio de control)*[2]. Hoy en día a 30 años de la reforma constitucional de 1994, dicho instituto es visto desde una mirada amplia y superadora. Ya no se vincula únicamente a la intimidad o la privacidad de las personas titulares de los datos personales, sino que, esto se modificó como resultado del gran procesamiento de datos que se dio inicialmente desde una perspectiva más analógica debido a el perfeccionamiento de la burocracia administrativa estatal y las entidades privadas encargadas de recopilar información, hasta el punto en que al día de hoy nos encontramos inmersos en un mundo completamente atravesado por el gran procesamiento de datos o mejor conocido como la “big data”¹. En este contexto, la irrupción de la informática ha implicado una revisión del derecho a la intimidad debido a la creación de extensas bases de datos de naturaleza personal y la capacidad de cruzar la información contenida en ellas. Como bien señala el Dr. Molina Quiroga *el derecho a la intimidad no podía seguir considerándose simplemente la ausencia de información acerca de nosotros en la mente de los demás (el “déjenme solo”), sino que debía adquirir el carácter de un control sobre la información que nos concerniera, o sea la facultad del sujeto de controlar la información personal que sobre él figurara en los bancos de datos* [3]. Por esta razón es que la mirada actual para la doctrina de este derecho supera la concepción tradicional de la protección vinculada a la intimidad, debido a que actualmente la vulneración de este tipo de información abarca no solamente a los datos públicos sino a

el honor, la identidad, la libertad, derechos de carácter económico, entre otros derechos. Por lo tanto, es reconocido como un derecho autónomo producto de la posibilidad de controlar la información de carácter personal que tiene el titular de los datos personales, mediante el uso de esta garantía constitucional como medio.

III. ¿QUÉ ES LA PROTECCIÓN DE DATOS PERSONALES?

Para comprender adecuadamente el alcance y la importancia de la protección de datos personales como un derecho fundamental, es esencial comenzar por definir qué constituye un dato personal en sí mismo. Los datos personales según el art. 2 de la ley 25.326 son aquella información de cualquier tipo referida a personas físicas o de existencia ideal, tanto determinadas como determinables. Por tanto, cuando nos referimos a un segmento de la realidad que constituye información, es decir, un dato, y este dato hace alusión a una persona física o jurídica, nos encontramos frente a lo que se denomina un dato personal. En este contexto, resulta relevante destacar que cualquier tipo de información que pueda estar relacionada con una persona, ya sea de forma directa o indirecta, se considera como dato personal. Es por esto que este tipo de información que suele ser almacenada por entidades públicas y privadas es de gran importancia a la hora de garantizar la protección de la información que almacenan. Aún más, la legislación al respecto establece que no es necesario que la persona esté completamente individualizada para que la información se considere como un dato personal, con el simple hecho de tener la posibilidad de poder identificarla mediante algún mecanismo técnico cumple con los requisitos para ser catalogada como tal. Podemos tomar como ejemplo una imagen de una persona, su dirección física o electrónica, número de teléfono, una nota de voz o cualquier otro tipo de información que pueda ser vinculada directa o indirectamente a un sujeto. Todos estos elementos debido a su vinculación o posible vinculación a un individuo son considerados datos personales. Es fundamental comprender que en la actual era digital, una gran cantidad de datos ya no se almacena en soportes analógicos. Estos datos están ampliamente dispersos y se guardan en una variedad de sistemas digitales alojados en servidores, que para el ordenamiento jurídico pueden ser considerados como bases de datos o bancos de datos, ya sea públicos o privados, dependiendo de la entidad o individuo que posea la titularidad de la información. Estos datos pueden ser utilizados para una amplia gama de propósitos, desde la prestación de servicios hasta la realización de análisis de mercado o incluso la prestación de servicios educativos como en el caso de las entidades educativas.

IV. PANORAMA ACTUAL DE LA PROTECCIÓN DE DATOS PERSONALES.

Si bien contamos con la consagración constitucional de la protección de datos personales esto no implica que la legislación actual que busca regular este derecho se encuentre

¹ El término “Big Data” se refiere al procesamiento de una gran cantidad de datos e información mediante el uso de herramientas digitales. Estas herramientas procesan Macrodatos que son una gran escala de información, de carácter compleja que precisa de un software informático específico para su procesamiento.

totalmente actualizada o alineada con los estándares internacionales, ni mucho menos adaptada a las cambiantes dinámicas que acompañan los avances vertiginosos de la tecnología. Es crucial reconocer que el mundo digital en el que vivimos está en constante evolución. Cada día, surgen nuevas tecnologías, aplicaciones y plataformas que transforman la manera en que interactuamos y compartimos información en sociedad. Este dinamismo tecnológico no solo nos brinda beneficios y oportunidades, sino que también plantea desafíos significativos en términos de protección de datos y privacidad. En este contexto, la legislación existente puede quedar rezagada o insuficiente para abordar los complejos escenarios que surgen del uso masivo de datos personales en línea, la proliferación de dispositivos conectados a internet, el desarrollo de tecnologías disruptivas como la inteligencia artificial y el aprendizaje automático e incluso las problemáticas que conlleva la cibercriminalidad. Es importante tener presente que la legislación que rige la protección de datos personales en Argentina fue promulgada a fines del año 2000, lo que implica que ha estado en vigencia por más de 20 años. Asimismo, es oportuno mencionar que la Constitución cumplió 30 años desde su última reforma, momento en el cual se incorporó este instituto a nivel constitucional. A la luz de este marco normativo, se percibe una proximidad temporal en su promulgación, pero en lo que respecta al avance tecnológico, se observa una distancia considerable.

Nos encontramos en un contexto que la vertiginosa realidad digital nos enfrenta con desafíos impensados. Podemos tomar como ejemplo los diversos casos de filtraciones de datos personales, como lo fue la reciente filtración del RENAPER, en donde se publicó una base de datos con 65 millones de registros de datos personales[4]. Estos tipos de delitos perpetrados son realizados por la ciberdelincuencia que opera de manera organizada y sofisticada, realizando ciberataques a organismos públicos y privados con el objetivo de exponer las vulnerabilidades de los países y poner la información obtenida al alcance del público. Estos acontecimientos eran algo impensado en el momento en que la Argentina decidió consagrar constitucionalmente la protección de datos personales. En aquel entonces, la Constitución y la posterior sanción de la Ley 25.326 no anticiparon la posibilidad de que los registros de todos los ciudadanos del territorio argentino pudieran quedar expuestos a cualquier persona con un solo click. Estos incidentes de filtración de información personal han suscitado un llamado de atención significativa por parte de los organismos públicos y privados que se ven afectados, así como también una consideración jurídica respecto a la responsabilidad estatal en este ámbito. Además, han intensificado el cuestionamiento sobre la idoneidad de la legislación vigente, reflejando la creciente preocupación entre los ciudadanos.

Es por esto que la actual ley de protección de datos personales se encuentra en un proceso de reforma llevado adelante por la Agencia de Acceso a la Información Pública que inició un proceso de debate participativo, abierto y transparente para la reforma de la Ley de protección de datos personales. Este proceso involucró la realización de mesas

preparatorias y mesas de diálogo con diversos sectores de la sociedad. Como resultado de este proceso de participación y debate, se elaboró una Propuesta de Anteproyecto. Posterior a esto se le dió inicio a la fase de consulta pública a raíz de la resolución 119/2022 y la posterior resolución 145/2022 que postergó el plazo del periodo de consulta.

En cuanto a los avances que si se pudieron lograr podemos mencionar la sanción de la ley 27.483, la cual tuvo por objeto la adhesión de la Argentina al Convenio 108 del Consejo de Europa sobre protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Este convenio representa un acuerdo internacional que establece pautas y principios para proteger los datos personales en el ámbito del tratamiento automatizado. Al ratificar este convenio, Argentina asume el compromiso de incorporar en su ordenamiento jurídico interno las disposiciones y principios estipulados en el mismo, con el fin de garantizar la protección de datos personales conforme a estándares internacionales reconocidos.

En lo que respecta a el objetivo del proceso de reforma legislativa es importante destacar que la finalidad principal es alinear las normativas nacionales de protección de datos personales con los estándares establecidos en normativas que son vanguardia como el caso del Reglamento General de Protección de Datos (GDPR) en Europa y la Ley General de Protección de Datos (LGPD) en Brasil. Estos marcos legales, reconocidos internacionalmente, establecen principios de protección robustos y mecanismos efectivos para garantizar la privacidad y seguridad de la información personal. Al lograr reformar nuestro marco jurídico y adecuar la legislación Argentina a estos estándares, se lograría fortalecer la protección de datos de los ciudadanos.

V. DELEGADO DE PROTECCIÓN DE DATOS PERSONALES.

Una vez conceptualizado el alcance de la protección de datos personales y su panorama actual es importante profundizar en cuanto a la figura del Delegado de Protección de Datos Personales[5].

El Delegado de Protección de Datos Personales es el elemento central del cumplimiento de las disposiciones de protección de datos personales[6]. En el caso de Argentina, contamos con la ley 25.326, que, si bien no contempla en su articulado esta figura, su reconocimiento surge en base a distintas resoluciones emitidas por la Agencia de Acceso a la Información Pública, autoridad de aplicación de dicha ley. Además, está contemplada esta figura por el Proyecto de Ley de Protección de Datos Personales como obligatoria para todo aquel que realice tratamiento de datos, más aún como sostiene en su art. 44 inc a) “Si se trata de una autoridad u organismo público”[7].

En cuanto a sus funciones es aquel responsable que tiene a su cargo ser un nexo entre la autoridad de protección y la organización en la que convive. Su labor consiste en ser el encargado de llevar adelante el programa de privacidad del organismo, el cumplimiento de la regulación de datos personales y facilitar que las organizaciones cumplan con

dichas regulaciones. Además de ser un asesor de opiniones jurídicas, analizar la manera en que se transfieren datos personales intencionalmente, realizar un registro activo del tratamiento de datos que se realice, etc. Dentro de sus funciones principales encontramos aquellas relacionadas a realizar monitoreo de riesgo, llevar adelante un inventario y acompañar el desarrollo de las evaluaciones de impacto sobre los datos personales. Llevan adelante constantes auditorías y monitoreos para ver si existen desvíos en el programa de protección que lleven adelante.

En cuanto a si surge alguna problemática con los datos que se traten como puede ser una filtración de datos alojados en una base de datos, el delegado y la organización tienen que llevar adelante un reporte de incidente de seguridad, debido a que esto puede afectar los datos personales de distintos particulares. Es necesario que se realice un reporte ante la autoridad de protección de datos y se comunique a todas las personas afectadas por el incidente de seguridad, incluso si este incidente no haya producido aun daño alguno. Se le debe explicar al afectado cuales son los pasos que adoptar para que el titular evite que se produzca un daño a causa de la filtración de datos. Por ejemplo, si una empresa pierde datos de una tarjeta de crédito se debe dar aviso para que se comuniquen con la empresa y realicen las gestiones necesarias para cambiar los datos.

Si bien estas cuestiones no son obligatorias en Argentina, son resultado de la aplicación de los estándares internacionales provenientes del GDPR (Reglamento de Protección de Datos Personales) y la ley de Brasil LGPD (Ley General de protección de Datos Personales), siendo este un punto a seguir que se ve hoy en día plasmado en nuestro proyecto de reforma de la ley 25.326 y las distintas resoluciones que emite nuestra autoridad de aplicación de la ley.

VI. IMPLEMENTACIÓN DEL DELEGADO DE PROTECCIÓN DE DATOS PERSONALES EN LAS UNIVERSIDADES.

Es reconocido que el Delegado de Protección de Datos Personales es una figura que suele predominar en el sector privado, a razón de que es un elemento esencial para actores que se dedican al tratamiento masivo de datos, sin embargo, debemos tener en cuenta la **Resolución 40/2018** de la Agencia de Acceso a la información Pública. Dicha resolución en sus considerandos sostiene que: “para la eficacia de la política de tratamiento de datos personales es conveniente recomendar a los organismos estatales que posean bases de datos, la designación de un agente de planta permanente como “delegado de protección de datos personales” a fin de que cumpla la tarea de acompañar la implementación y control del cumplimiento de la política de protección de datos personales que se diseñe”. Es por esto por lo que en su Art. 3 recomienda la designación de un agente bajo estos supuestos y aún más en el ANEXO 1 utilizado como “POLÍTICA MODELO DE PROTECCIÓN DE DATOS PERSONALES PARA ORGANISMOS PÚBLICOS” contempla en su modelo la posibilidad de contar con una línea directa de contacto con estos agentes para que pueda cumplir con su tarea. Debemos

tener en cuenta entonces que si bien hoy en día en nuestro ordenamiento jurídico no es de carácter obligatorio la figura del Delegado de Protección de Datos Personales y tampoco lo es realizar tareas preventivas ante un incidente de seguridad sobre una base de datos personales, podría implementarse dicho actor en las políticas de protección de la información que diagramen los organismos públicos.

A la luz de esta resolución, resulta pertinente cuestionar si es adecuado implementar esta figura en las universidades nacionales. Por ende, es fundamental referirse a la Ley de Educación Superior, que regula la educación superior en Argentina. Dicha ley define los niveles y modalidades de la educación superior, incluyendo universidades, institutos universitarios y establecimientos de formación técnica y profesional. Asimismo, en su artículo 29 garantiza y consagra la autonomía de las universidades nacionales en cuanto a la gestión académica, administrativa y económica, permitiendo a su vez a las universidades definir sus planes de estudio, políticas de investigación y designación de autoridades.

En relación con este asunto, es importante señalar que las universidades, en virtud de su autonomía, tienen la capacidad de decidir si desean adaptarse a la resolución mencionada e implementar la figura del Delegado de Protección de Datos Personales. Esta decisión les permitiría establecer un agente encargado de velar por el cumplimiento de las normativas de protección de datos, garantizando así la seguridad y confidencialidad de la información sensible que manejan, tanto del alumnado como del personal universitario.

Aunque es sabido que en muchos organismos ya existen responsables designados para la seguridad de la información, esto no significa que sus funciones y responsabilidades se equiparen a las de un Delegado de Protección de Datos Personales. Los encargados de seguridad de la información suelen centrarse en la protección técnica y operativa de los sistemas, es decir, en garantizar que la infraestructura tecnológica sea segura y que los datos estén resguardados frente a amenazas externas, como ciberataques o fallos en la seguridad informática. Sin embargo, un delegado de protección de datos tendría un alcance más amplio y responsabilidades específicas que van más allá de la simple seguridad técnica. Este agente estaría encargado de asegurar el cumplimiento de las normativas sobre protección de datos personales, supervisando que los procesos de recolección, almacenamiento y tratamiento de la información se realicen de acuerdo con la legislación vigente. Además, tendría la obligación de velar por los derechos de los titulares de los datos, garantizando que se respeten principios como la confidencialidad, el consentimiento informado y el derecho a la rectificación o eliminación de la información cuando sea necesario. En este sentido, si en el futuro se llevara a cabo una reforma legislativa que incorporara formalmente la figura del Delegado de Protección de Datos Personales, y esta se convirtiera en una obligación derivada de una ley nacional, las responsabilidades de este agente estarían claramente definidas por dicho marco legal. Esta normativa podría establecer de manera precisa los alcances de su actuación, incluyendo las medidas de protección a implementar, las sanciones aplicables por el incumplimiento de sus obligaciones y la relación directa que tendría con las

autoridades de control en materia de datos personales. Este tipo de regulación podría cambiar sustancialmente el panorama actual, exigiendo a los organismos públicos y privados, incluidas las universidades y otras instituciones educativas, la designación de un Delegado de Protección de Datos Personales con funciones específicas y detalladas. De esta manera, se fortalecería el marco de protección de los datos personales, asegurando un tratamiento más riguroso y transparente de la información en diversos ámbitos, particularmente en aquellos que manejan grandes volúmenes de datos sensibles como el sector educativo.

Un ejemplo claro de esta situación se observa en España, donde universidades como la Universidad Autónoma de Madrid (UAM) han implementado la figura de un responsable para el tratamiento de datos personales en todas las actividades y servicios que brindan. Esto se enmarca en lo establecido por el Reglamento General de Protección de Datos, el cual exige que las instituciones que gestionan información personal adopten medidas de protección adecuadas.

Siendo así que en cumplimiento de lo dispuesto en el artículo 37.5 del Reglamento General de Protección de Datos, la UAM designó a Jesús Larena Millán como Delegado de Protección de Datos el 21 de diciembre de 2021[8]. El Delegado de Protección de Datos Personales desempeña un rol crucial dentro de la universidad, con responsabilidades que abarcan desde asesorar e informar a la institución sobre las mejores prácticas en el tratamiento de datos personales, hasta supervisar que los procedimientos internos cumplan con la normativa vigente en materia de protección de datos.

Además, el Delegado de Protección de Datos es un punto de referencia esencial para toda la comunidad universitaria. Su papel incluye atender las consultas de estudiantes, docentes y personal administrativo en lo que respecta a la protección de datos, así como facilitar el ejercicio de los derechos que otorga el RGPD, tales como el derecho al acceso, rectificación, supresión y oposición al tratamiento de datos. Asimismo, el Delegado de Protección de Datos Personales tiene la misión de concientizar y formar al personal de la universidad, fomentando una cultura de protección de la privacidad y la seguridad de la información dentro de la institución. Por último, es importante destacar que dicha figura colabora activamente con la Agencia Española de Protección de Datos (AEPD), actuando como enlace entre la universidad y la autoridad de control, lo que asegura que la UAM no solo cumpla con las normativas nacionales e internacionales, sino que también responda adecuadamente ante cualquier incidencia relacionada con la gestión de datos personales. Este ejemplo pone de manifiesto cómo las universidades pueden adaptarse a las normativas internacionales para proteger eficazmente la información de su comunidad.

VII. CONCLUSIONES:

En virtud de lo expuesto es destacable mencionar que la protección de datos personales se ha afirmado como un derecho fundamental en Argentina, especialmente desde su inclusión en el artículo 43 de la Constitución Nacional durante

la reforma de 1994. Inicialmente asociado con el derecho a la intimidad, este derecho ha evolucionado significativamente con el avance tecnológico y la expansión de la "big data". La necesidad de proteger la información personal ha adquirido una dimensión más amplia, abarcando no solo la privacidad sino también la seguridad y el control de la información en un entorno digital en constante cambio. El concepto de protección de datos personales ha sido impulsado por la creciente sofisticación del procesamiento de información y la formación de grandes bases de datos, lo que ha llevado a una revisión de cómo entendemos la privacidad. Hoy en día, la protección de datos personales no abarca solamente la protección de la intimidad, sino que se extiende hasta incluso la capacidad de controlar cómo se recopilan, almacenan, y utilizan los datos personales. Esta evolución se refleja en el reconocimiento del derecho a controlar la información personal en una era de procesamiento masivo y tecnologías avanzadas. En este contexto, el Delegado de Protección de Datos Personales juega un rol crucial. Aunque la Ley 25.326, no menciona explícitamente esta figura, su importancia ha sido reconocida a través de diversas resoluciones de la Agencia de Acceso a la Información Pública y el Proyecto de Ley de Protección de Datos Personales. Según estas normativas, el Delegado de Protección de Datos Personales es una figura clave para asegurar el cumplimiento de las regulaciones de protección de datos y facilitar la implementación de políticas adecuadas en la organización. El Delegado de Protección de Datos Personales actúa como un puente entre la organización y la autoridad de protección de datos, gestionando el programa de privacidad de la entidad y supervisando el cumplimiento de las normativas. Además, el Delegado de Protección de Datos Personales debe facilitar el ejercicio de derechos por parte de los titulares de los datos y colaborar estrechamente con la autoridad de protección para resolver cualquier incidencia relacionada con la gestión de la información personal. A nivel internacional, el papel del Delegado de Protección de Datos Personales ha sido adoptado con éxito por diversas instituciones. Un ejemplo destacado es la Universidad Autónoma de Madrid (UAM), donde se ha implementado un Delegado de Protección de Datos Personales para asegurar el cumplimiento del Reglamento General de Protección de Datos. En el ámbito argentino, aunque la figura del Delegado de Protección de Datos Personales no es actualmente obligatoria, la Resolución 40/2018 de la Agencia de Acceso a la Información Pública, autoridad de aplicación de la ley 25.326, recomienda su designación para organismos públicos con bases de datos. Esta recomendación refleja la importancia de contar con un profesional especializado en la protección de datos, especialmente en un contexto donde las filtraciones de datos y los incidentes de seguridad son cada vez más comunes. La posibilidad de implementar un Delegado de Protección de Datos Personales en las universidades nacionales debería alinearse con la autonomía que les otorga la Ley de Educación Superior. Esta ley permite a las universidades definir sus políticas internas y gestionar de manera efectiva la protección de la información que manejan. La inclusión de un Delegado de Protección de Datos Personales podría no solo reforzar la seguridad de los datos personales de estudiantes y personal, sino también mejorar el cumplimiento de los

estándares internacionales en protección de datos. En conclusión, la implementación de un Delegado de Protección de Datos Personales en las universidades nacionales representa una posibilidad de lograr alinear a las casas de estudio con las mejores prácticas internacionales. Aunque no es una obligación legal en Argentina en este momento, la adopción de esta figura podría fortalecer significativamente el marco de protección de datos, garantizando una gestión más rigurosa y transparente de la información personal. Esta medida sería un paso hacia una mayor protección de la privacidad en el ámbito educativo, reflejando un compromiso con los derechos de los individuos y adaptándose a los desafíos contemporáneos en el manejo de datos personales.

REFERENCIAS

- [1] Palazzi Pablo. Protección de Datos Personales: Doctrina y Jurisprudencia. Tomo 1. Oscar R. Puccinelli. La ley N° 25.326, de cara a su reforma integral: el proyecto elaborado en el marco del Programa Justicia 2020. CDYT. Buenos Aires. (2021). Pag 56.
- [2] Quiroga Lavié, Derecho Constitucional Argentino. Rubinzal-Culzoni. (2001). Pág. 150.
- [3] Eduardo Molina Quiroga. Protección de datos personales como derecho autónomo. Principios rectores. Informes de solvencia crediticia. Uso arbitrario. Daño moral y material. SAIJ. (2003). Pag 3.
- [4] Disponible en: https://www.clarin.com/tecnologia/filtraciones-datos-personales-demandan-responsabilidad-discuten-ley-vigente_0_2g8DEGGLMa.html. Último acceso 30/8/2024.
- [5] GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS Creado por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995. ARTÍCULO 29: Directrices sobre los delegados de protección de datos (DPD). Pag 4.
- [6] GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS Creado por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995. ARTÍCULO 29: Directrices sobre los delegados de protección de datos (DPD). Pag 4.
- [7] https://www.argentina.gob.ar/sites/default/files/proyecto_de_ley_de_proteccion_de_datos_personales_-_febrero_2023.pdf
- [8] Disponible en: <https://www.uam.es/uam/proteccion-datos/delegado-proteccion-datos>. Último acceso en 30/8/2024.