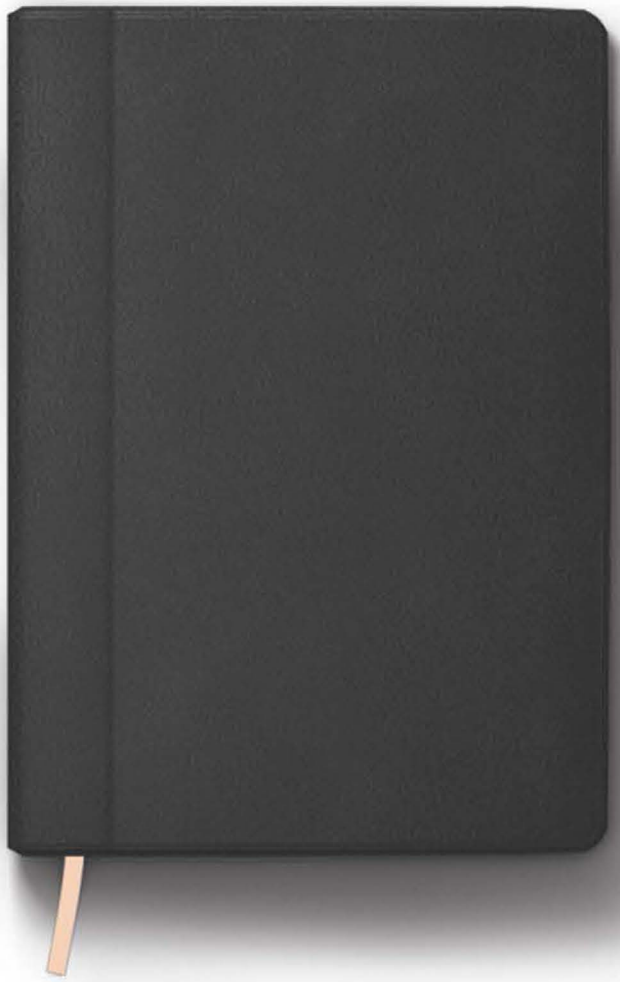
CUADERNOS DE POSGRADO 2024

SECRETARÍA DE POSGRADO



FACULTAD DE DERECHO
Y CIENCIAS SOCIALES Y POLÍTICAS
UNIVERSIDAD NACIONAL DEL NORDESTE

UNIVERSIDAD
NACIONAL
DEL NORDESTE

Cuadernos de Posgrados

| 2024 |

Cuadernos de posgrados 2024 / Carla Camila Jarko ... [et al.] ; Compilación de Mónica Andrea Anís ; Director Nahuel Pellerano ; Hilda Zulema Zárate. - 1a ed adaptada. - Corrientes : Universidad Nacional del Nordeste. Facultad de Derecho y Ciencias Sociales y Políticas, 2025.
Libro digital, PDF

Archivo Digital: descarga y online
ISBN 978-631-6623-11-9

1. Derecho. I. Jarko, Carla Camila II. Anís, Mónica Andrea, comp. III. Pellerano, Nahuel, dir. IV. Zárate, Hilda Zulema, dir.
CDD 346.02

“El delegado de protección de datos en el comercio electrónico”

| Eduardo Arturo Claudiani |

»

Introducción

En el presente trabajo se pretende realizar un breve análisis de lo que implican los datos en el comercio electrónico. Sus características y particularidades. La importancia de los mismos. El manejo, tratamiento, resguardo y protección de datos. Su regulación local e internacional. El sistema europeo de datos. Y en especial, la figura del Delegado de Protección de Datos, recientemente implementado por la AFIP en nuestro país.

Sabemos que la información es la principal protagonista de los enormes cambios socioeconómicos que estamos experimentando. Estamos asistiendo a una revolución tecnológica que viene transformando el modo de vida de millones de personas y provocando cambios muy significativos en la comunidad global. Lo que se llama la Cuarta Revolución Industrial. Y que está cambiando la forma de vivir, trabajar y relacionarnos entre las personas, y que por su magnitud y complejidad es algo inédito en la experiencia de la humanidad.

Esta cuarta etapa está caracterizada por la interrelación de avances tecnológicos que abarcan una gran cantidad de campos, incluyendo inteligencia artificial, robótica, internet de las cosas, tecnología blockchain, nanoteconología, biotecnología, computación cuántica, impresión 3D, la ciencia de materiales, el almacenamiento de energías y vehículos autónomos. Se tiene dicho que tanto la Tercera, como la Cuarta Revolución Industrial comparten el mismo recur-

so estratégico: la información y el conocimiento. La materia prima de la industria 4.0 son entonces los datos, siendo la información el motor de la economía, y como tal, uno de los activos más importantes de las organizaciones.

Pero, al mismo tiempo que podemos mencionar muchísimos aspectos positivos de la relevancia que tiene la información para la vida moderna, también es imperioso prestar especial atención a los aspectos negativos que su uso intensivo, descontrolado y desmedido puede llegar a implicar. Tales desarrollos tecnológicos, que por un lado generan enormes beneficios para la sociedad, por otro lado, traen también nuevos desafíos a la privacidad, obligando a redefinirla, protegerla y reglamentarla. La enorme capacidad de procesar datos es tanto una bendición como una maldición, ya que permite encontrar soluciones casi instantáneas a los problemas, pero al mismo tiempo inmiscuirse con la misma facilidad en la intimidad de las personas. Y eso lleva a un tercer aspecto negativo que es el déficit de confianza que genera el uso irresponsable de los datos en la opinión pública, lo que también merece atención y tratamiento.

Veremos a continuación algunos aspectos vinculados a tales cuestiones, y concretamente la figura del Delegado del Protección de Datos, como objetivo del presente trabajo.

Desarrollo

Regulación Local en Materia de Datos:

En nuestro país está vigente la Ley Nro. 25.326 referente a la protección de datos personales, que como principal crítica está el hecho de que fue sancionada hace 24 años, por lo cual merecería una urgente actualización. La misma establece una clasificación acerca de los datos, viendo que existen los: a) datos personales; y b) datos sensibles. Los primeros refieren a la información de cualquier tipo referidas a personas físicas o de existencia ideal, resultando que el dato personal

se formará de un dato informático procesado para extraer la información que éste contiene. Los datos sensibles, por su parte, son los 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. Siendo el dato personal el género y el sensible la especie.

Según el art. 1 de la ley su objeto es la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, públicos o privados, destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre estas se registre, conforme lo establecido por el art. 43, párrafo tercero de la Constitución Nacional.

El Reglamento Europeo de Protección de Datos, y en los países de Latinoamérica:

En Europa, por su parte, comenzó a regir en el año 2018 el Reglamento General de Protección de Datos, que tiene como característica su aplicación obligatoria a cualquier compañía, persona o empresa que se encuentre tanto en la Unión Europea, como fuera de ella, y que afecte a algún ciudadano europeo. Por lo tanto, si una plataforma de comercio electrónico situada en nuestro país, obtiene, registra y procesa datos de algún ciudadano europeo, debería cumplir con el RGPD.

En el marco de ese reglamentó, en Europa se creó la figura del Delegado de Protección de Datos, que es la persona o ente encargado o responsable de supervisar cómo se tratan los datos personales, y de informar y aconsejar a los que tienen dicha tarea, sobre las obligaciones legales vigentes. Teniendo previstas multas muy significativas para el caso de incumplimiento. Esta figura no estaba contemplada en nuestra reglamentación, pero recientemente fue implementada por el AFIP mediante Disposición Nro. 173/2024, que se analizará más adelante.

Otra característica que diferencia al sistema europeo con el existente en nuestro país, es la plena vigencia y operatividad del derecho al olvido, como obligación de las plataformas de borrar aquella información perteneciente a la vida privada de las personas. En nuestro país tuvimos el resonante caso "De Negri", que si bien tuvo acogida favorable en Primera y Segunda Instancia, luego la CSJN se expidió priorizando el "derecho a la información", por sobre el "derecho al olvido". Y con ello, abriendo un debate en cuanto a la posible responsabilidad de las plataformas por el uso o manipulación de los datos.

El Reglamento General produjo un impacto en Latinoamérica llevando a un proceso de reformas de las legislaciones vigentes para adecuarlas al nuevo estándar europeo. Ya que el Reglamento establece trabas para exportar datos de ciudadanos comunitarios a países con regulaciones de privacidad que no sean consideradas adecuadas, compeliendo a los mismos a mantener un estándar similar al europeo en dicha materia. Argentina, Chile, Costa Rica y Uruguay comenzaron con sendos procesos de reformas con distintos grados de avance. Brasil, por su parte, sancionó la Lei Geral de Protecao de Dados Pessoais, que es considerada como la legislación latinoamericana más similar al reglamento europeo.

La Responsabilidad Proactiva:

Una de las contribuciones más importante del reglamento europeo es la creación del concepto de *accountability* al mundo del *compliance* en protección de datos, que está siendo replicado por la mayoría de las regulaciones más modernas. El concepto de *accountability* es de difícil traducción en una sola palabra al español, pero puede entenderse como "responsabilidad", "rendición de cuentas" y "compromiso", al mismo tiempo.

La legislación Colombiana lo denomina "responsabilidad demostrada", los proyectos de reforma de Argentina, Chile y Uruguay, "responsabilidad proactiva", mientras que en Brasil se la denomina

"responsabilización y prestación de cuentas". Más allá del nombre, el accontability implica un cambio de paradigma en el campo del cumplimiento regulatorio en privacidad. La responsabilidad proactiva obliga a las organizaciones a adoptar medidas que le permitan demostrar que no solo "cumple" con la ley, sino también "cómo" lo hace; debe poder demostrar "la manera" en que cumple la ley. Y los beneficios para los titulares de los datos. Demostrar "cómo" el cumplimiento de la ley beneficia al interesado es mucho más importante que simplemente cumplir con la obligación. En el ámbito de Latinoamérica se está comenzando a incorporar el principio de la responsabilidad proactiva de a poco.

Y esa tarea, de incorporar responsabilidad proactiva al programa de privacidad por parte de una organización, se traduce en: 1) demostrar cómo se cumple; 2) inventario de actividades de procesamiento de datos; 3) privacidad desde el diseño; 4) evaluación de impacto en la protección de datos; 5) reportes de incidentes de privacidad; y finalmente 6) designar un delegado de protección de datos.

El Delegado de Protección de Datos:

Este funcionario no es directamente responsable por el cumplimiento de la ley, sino que es el asesor de la organización, la persona que facilita el cumplimiento regulatorio. La responsabilidad por el cumplimiento de la regulación de protección de datos pesa sobre toda la organización, en la que cada colaborador es responsable por cumplir con la ley en cada procesamiento de dato que realice para la misma.

El DPO tiene a su cargo coordinar la actividad y los procesos de la organización para alcanzar la adecuación a las regulaciones de protección de datos. En la práctica, debe ser un aliado estratégico de todas las áreas de la organización, que desarrolla soluciones pragmáticas y sostenibles que respetan la protección de la información personal al tiempo que apoyan la innovación y el cumplimiento de los objetivos de la organización.

También debe constituirse en un administrador de riesgos estratégicos, que crea estándares y controles simples y efectivos que le permiten a laorganización seguir los principios de privacidad y cumplir con las reglas de protección de datos. Promover una sólida cultura de privacidad dentro de la organización que genere compromiso y sensabilización sobre su importancia.

Las habilidades y características que debe reunir el DPO son: a) experticia legal en materia de protección de datos; b) conocimiento de tecnología, para detectar los desafíos a la privacidad que pueden provocar; c) pensamiento innovador para permitir el cumplimiento de los objetivos de la organización y al mismo tiempo garantizar el cumplimiento regulatorio; d) gestión de riesgos, que le permita identificar los mismos, medir la efectividad de los controles y evaluar el riesgo residual; e) capacidad pedagógica para fomentar una cultura de protección de datos; f) sensibilidad cultural y habilidades comunicacionales para generar compromiso interno sobre privacidad; g) coraje profesional para oponerse a aquellos procesos o iniciativas que impliquen un riesgo inaceptable a la privacidad de los titulares de los datos.

El Delegado de Protección de Datos en la Argentina:

Como dijimos, nuestra Ley de Datos Personales Nro. 25326, que data del año 2000, no incorpora la figura del Delegado de Protección de Datos, figura que no se estaba aplicando ni incorporando en los distintos organismos.

Recientemente, sin embargo, la Administración Federal de Ingresos Públicos (AFIP) mediante el dictado de la Disposición Nro. 173/2024 designó un Delegado de Protección de Datos, convirtiéndose así en el primer organismo público del país en introducir un avance tan significativo y necesario para el cumplimiento y control de la normativa de protección de datos personales.

En nuestro país son conocidos y tratados con honda preocupación los constantes incidentes de seguridad y filtraciones de información

sensible que sufre el sector público, afectando gravemente los derechos de las personas cuyos datos constan en ellos. Por lo que, era largamente reclamada la necesidad urgente de implementar la figura del DPO en nuestro país. La Disposición Nro. 173/2024, en su parte dispositiva, designa en la persona del abogado Eduardo Hernán Cimato la función de "delegado de protección de datos personales" de dicho organismo (art. primero); encomendar al mismo a impulsar, con intervención de las áreas competentes, la implementación de la Política de Protección de Datos Personales, y entender en su difusión y en el control de su cumplimiento. Entre sus considerandos menciona que en su artículo segundo de la Ley 25.326 define al archivo, registro, base o banco de datos, como el conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

Que la Agencia de Acceso a la Información Pública, como autoridad de control y aplicación de la Ley 25.326, de acuerdo con lo prescripto por el artículo 19 de la Ley Nro. 27.275, a través de la Resolución Nro. 40 del 04 de julio de 2018 (AAIP) aprobó el documento intitulado "POLITICA MODELO DE PROTECCIÓN DE DATOS PERSONALES PARA ORGANISMOS PÚBLICOS", como pauta básica sugerida para el diseño del documento que publicite la protección que a tales datos les confieren los organismos públicos titulares de bases de datos personales. Que en la citada resolución, la Agencia recomendó a los organismos estatales titulares de bases de datos titulares la implementación de una política de protección de datos personales, su difusión en forma permanente y actualizada y la designación de un delegado de datos personales.

Así, la AFIP, en su condición de titular de base de datos personales, y en atención a la recomendación efectuada por la AAIP, entendiendo que un DPO contribuirá a fortalecer la transparencia en la gestión de los datos personales, consideró conveniente designar a un agente de planta permanente en tal carácter, encomendándole ocuparse de los cometidos previstos por la Resolución Nro. 40/18 (AAIP).

Los beneficios en tal sentido pueden enumerarse en: mayor transparencia y confianza de los ciudadanos en el manejo de su información tributaria; prevención y mitigación de posibles brechas de seguridad; ubica al organismo a la vanguardia en el cumplimiento de las normativas de protección de datos; promover una cultura en tal sentido dentro de la organización.

Naturalmente, dado el carácter novedoso de la implementación de dicho instituto, el mismo no estará exento de grandes desafíos, continua capacitación y actualización para estar a la altura de las novedades y evoluciones tecnológicas y normativas en dicho campo.

Sin embargo, la designación de un primer DPO en un organismo público argentino marca un hito en la historia de protección de datos en el país, que a mi criterio y además de cumplir con expectativas altamente esperadas y establecer un estándar para otras instituciones, implicará un mayor grado de seguridad y confianza en los titulares de datos, personas físicas y jurídicas, sumamente necesario en los tiempos actuales. Se celebra grandemente dicha novedosa incorporación, y se espera sea emulada rápidamente.

Conclusiones

Dentro del contexto que se viene tratando, en lo referente a la necesidad imperiosa de una protección adecuada, eficiente y constante de los datos, considero que debe mencionarse los siguientes aspectos particulares, que en criterio del suscripto revisten mucho valor en la consideración de los particulares y empresas. Ellos, como herramientas coadyuvantes y de implementación conjunta con el DPO: La landing de privacidad, el panel de control de privacidad (que entre otras funciones permita contactar con el DPO), configuración de las preferencias de comunicaciones, gestión del consentimiento de "cookies", registro del historial de publicaciones visitadas; preferencias de recepción de publicidad personalizada. Por razones de extensión del

trabajo, me limito a mencionar estas herramientas, a las que les atribuyo suma importancia, a modo de apreciación personal, luego de haber estudiado el tema.

De todo lo visto, puede extraerse que tanto en nuestro país como a nivel mundial existe cada vez más concientización de la necesidad de incorporar prácticas y comportamientos que permitan a las organizaciones utilizar las tecnologías de una manera social, económica y ambientalmente responsable.

Ello no solo protege los derechos de los usuarios, sino que les da mayor seguridad y tranquilidad al momento de interactuar con dichas nuevas tecnologías. Y desde el otro extremo, implica un beneficio para las empresas, organismos y corporaciones que pretenden mantenerse competitivas y sustentables. Por ello es fundamental la implementación de un programa de privacidad que no se limite únicamente al cumplimiento de los postulados de la ley, sino que se gestione de manera continua y permanente para mejorar dinámicamente su eficacia.

En ese cometido, la función del DPO es primordial. Y por ello, celebramos su reciente incorporación según reglamentación mencionada, por parte de la AFIP, uno de los organismos más importantes como titular de bases de datos personales. Y entendiendo y esperando que a la brevedad sea imitado cada vez más por los distintos entes y organismos estatales, empresas y corporaciones que administren datos personales.

Bibliografía

1.-E-commerce. Aspectos Legales – Fernando Branciforte – La regulación y evolución de Internet. Consideraciones jurídicas completas, importantes para la actuación profesional. Ediciones dyd – innovación profesional – Año 2023.
2.- Daños en los Entornos Digitales – Jorge Mario Galdós – Ezequiel Valicenti – Tomo II – Santa Fe – Rubinzal – Culzoni - Año 2023.
3.- La Disposición Nro. 173/2024.