Universidad de
SanAndrés

Universidad de San Andrés

Escuela de Administración y Negocios

Magíster en Gestión de Servicios Tecnológicos y de Telecomunicaciones

PROTECCIÓN DE DATOS PERSONALES EN PERFILADOS Y DECISIONES AUTOMATIZADAS EN ARGENTINA

TESISTA

Agustina Sirvén

DNI 31.685.558

DIRECTOR DEL TRABAJO DE GRADUACIÓN

Enrique Hofman

Ciudad Autónoma de Buenos Aires, Agosto 2021.

AGRADECIMIENTOS

A Santiago y Mónica, sin quienes nada de esto hubiese sido posible.

A Eduardo Bertoni, por abrirme las puertas al trabajo diario en protección de datos y guiarme con este trabajo.

RESUMEN

En la actualidad, las organizaciones adoptan cada vez con mayor frecuencia como parte de su estrategia empresarial, distintas técnicas de marketing digital que implican tratamientos automatizados de la información, a través de perfilados y decisiones automatizadas. A menudo, estos mecanismos están generando efectos jurídicos negativos sobre derechos fundamentales de los usuarios.

Dada la necesidad de asegurar ciertos estándares de privacidad ante posibles afectaciones y la falta de una Ley actualizada en materia de protección de datos personales en Argentina -como el Reglamento Europeo de Protección de Datos Personales-, el objetivo de este estudio es determinar si, existen elementos jurídicos que habiliten en la actualidad a los usuarios afectados por estos tratamientos, a interponer un reclamo ante las empresas, o bien solicitar asistencia a la autoridad de control, es decir la Dirección Nacional de Protección de Datos Personales en el ámbito de la Agencia de Acceso a la Información Pública (AAIP).

Para tener una visión más acabada de estos mecanismos, se analizarán las técnicas más frecuentes de marketing digital en ámbitos empresariales y las categorías de datos de procesamiento, y se tendrán en consideración casos de derecho comparado donde se dieron efectos jurídicos negativos a raíz de perfilados y decisiones automatizadas. Se describirá el principal articulado del Reglamento Europeo de Protección de Datos (RGPD) y sus efectos, en comparación con la normativa nacional y la relevancia del rol del deber de información para el ejercicio y tutela de estos derechos.

De lo observado se desprende que, del marco regulatorio nacional se derivan los principales pilares para garantizar el ejercicio de estos derechos. No obstante, se detecta un incumplimiento generalizado de empresas al deber de información en sus Políticas de Privacidad lo que en principio, dificultaría su cumplimiento efectivo.

Asimismo, las dificultades de implementación del RGPD a nivel global, evidencian que la sanción de una ley actualizada en Argentina, si bien resulta deseable, no será suficiente por sí sola para proteger los datos personales ante este tipo de tecnologías tan avanzadas.

PALABRAS CLAVE

Decisiones automatizadas, perfilados, protección de datos personales, afectaciones a derechos fundamentales, normativa jurídica vigente en Argentina, ejercicio y tutela de derechos, organizaciones, autoridad de control.

ÍNDICE

CAPÍTULO 1. INTRODUCCIÓN

Según el economista Arthur, W. B. (1995) en la actualidad se dan infinidad de decisiones completamente automáticas en las organizaciones, lo que ha generado el fenómeno de una "segunda economía", caracterizada por ser "vasta, silenciosa, conectada, invisible y autónoma". Un enfoque más optimista de otro reconocido economista, Rifkin, J. (2014), concibe “el procomún colaborativo” como un nuevo paradigma de economía, que ofrece la posibilidad de reducir las diferencias en ingresos, democratiza la economía mundial y crea una sociedad más sostenible.

Lo que es indiscutible es que la economía digital trajo aparejado el procesamiento global de datos personales a través de múltiples técnicas de big data, resignificando para siempre el derecho fundamental de la privacidad, ahora asociado a valor económico de las organizaciones, mediante acepciones como el “petróleo del siglo XXI” o como la “columna vertebral” de los modelos de negocios.

En este contexto, no es novedad que la primera fase de digitalización estuvo caracterizada por la globalización de las operaciones de procesamiento de datos personales y que la analítica de éstos ha redefinido por completo la estrategia empresarial en la forma de adquirir nuevos clientes, retener a los existentes, entender las necesidades de productos y servicios, mejorar el valor agregado y fortalecer la competitividad.

Es evidente que las técnicas de marketing digital han jugado un rol clave en esta transición acompañando la transformación digital y cultural en las organizaciones. Así de un marketing masivo tradicional se ha ido avanzando hacia un “marketing relacional”, que permitía ir midiendo más acabadamente el rendimiento de las campañas de publicidad.

Hoy transitando la segunda fase de digitalización en 2021, estas técnicas han evolucionado hacia un marketing 5.0, donde el eje de la publicidad es la personalización “one to one” de los anuncios, alimentada por macrodatos, metadatos, inteligencia artificial y aprendizaje automático.

En este contexto, el COVID-19 como problemática global emergente, obligó a trasladar la presencialidad humana a la virtualidad, incrementado exponencialmente la demanda de consumo de productos y servicios a distancia, circunstancias que aceleraron los procesos de adopción de estas nuevas tecnologías en organizaciones.

En este orden de cosas, durante el año 2021 ya son varias las empresas que están experimentado el cambio organizacional de adopción generalizada de IA con operaciones de elaboración de perfiles y decisiones automatizadas para la personalización de oferta de sus productos y servicios.

1.1. PROBLEMÁTICA

La transición hacia una segunda fase de digitalización en organizaciones, despierta preocupaciones principalmente basadas en el hecho que durante la primera fase (es decir, desde la irrupción de las tecnologías de información), no se observó una cultura empresarial que pusiera prioridad a la protección de la privacidad de los usuarios.

Por el contrario, esta etapa estuvo caracterizada por la creencia empresarial que la adopción de mayores recaudos equivaldría a obligaciones excesivamente onerosas; y además, por la ausencia de una legislación que acompañara adecuadamente la evolución de estas innovaciones.

Hoy día, las organizaciones para respaldar las opciones de orientación de anuncios, tienen la capacidad de dirigirse a individuos sobre la base de una amplia gama de criterios de focalización. Tales criterios se desarrollan sobre la base de datos personales que los usuarios han proporcionado, han compartido activamente o bien, que han sido observados y/o inferidos por terceras partes.

Estas circunstancias están impactando en los derechos fundamentales, adquiriendo dimensiones más críticas y de mayor alcance, las que se traducen finalmente en las posibilidades de desarrollo de las personas, como de las distintas naciones.

Hacia “fuera” de la organización, resulta preocupante la tendencia generalizada de incumplimiento al Principio de de la Información en las Políticas de Privacidad de las empresas, al comunicar las condiciones que regirán el tratamiento y procesamiento de datos personales en el marco de la relación contractual a distancia que los une con los usuarios. En la mayoría de los casos, la falta de transparencia está dada por vicios en la información brindada, lo que influye en el ejercicio de derechos básicos, como en la tutela jurídica efectiva en cada jurisdicción nacional.

Hacia “dentro de la organización”, inquieta la falta de responsabilidad proactiva en la gestión de la información y el avance acelerado del desarrollo de actividades de procesamiento automatizado.

Muchas empresas realizan perfilados y predicciones, sin embargo, luego tienen dificultades para reconocer las salvaguardas a las que están obligadas. Las actividades de predicción significan la inferencia de nuevos datos personales y el perfilado, la clasificación de individuos, orientación de productos/servicios a individuos o grupos, análisis comportamental (evaluación y calificación de emociones, estados de ánimo, hábitos, preferencias, otros), los que indudablemente pueden impactar directamente o indirectamente en derechos fundamentales y libertades.

Estas operaciones, están implicando riesgos altos de procesamiento de datos sensibles o categorías especiales como: la igualdad, la no discriminación, la vida, la libertad religiosa, libertad personal, intimidad personal y familiar, propia imagen, expresión información, libre acceso a cargos y funciones públicas en condiciones de igualdad, tutela judicial efectiva, legalidad penal, educación, libertad de sindicación, derecho de petición, entre otros.

El alto impacto de estos procesamientos está asociado a daños significativos morales y materiales.

Es notorio que si no se garantizan determinados estándares de privacidad, estas nuevas tecnologías pueden entrañar riesgos para derechos y libertades

fundamentales, ya que en muchas ocasiones, las personas no son conscientes que se está creando un perfil o tomando decisiones sobre ellas.

Ante estas problemáticas, y con la necesidad de una regulación modernizada que brinde mayores garantías a los titulares de datos, el Reglamento General de Protección de Datos de la Unión Europea (en adelante, el "Reglamento" o "RGDP"), ha incorporado la protección frente a los casos de "valoraciones personales automatizadas" o elaboración de perfiles que pudieran provocar efectos jurídicos negativos a los titulares de datos, dándole el derecho a los interesados a oponerse a ser objeto de una decisión basada únicamente en el tratamiento automatizado de datos, y además, solicitarle al responsable de la base de datos una explicación sobre la lógica aplicada, solicitar intervención humana, e impugnar determinada decisión.

Ahora bien, al considerar el contexto normativo a nivel nacional en Argentina se advierte que, la Ley Nacional de Protección de Datos Personales posee más de veinte años desde su sanción, y que si bien se ha presentado un Anteproyecto de Ley (2017) ante el Congreso Nacional para su actualización, esta normativa ha perdido estado parlamentario en el año 2019. Durante 2020, se ha presentado un segundo Proyecto (2018), que principalmente ha tomando como base al anterior, el que actualmente continúa a estudio en el Congreso de la Nación.

1.2. PREGUNTAS DE INVESTIGACIÓN

Dada la necesidad de asegurar ciertos estándares de privacidad ante el creciente uso de estas herramientas de automatización de datos personales, ¿existen elementos jurídicos en la normativa vigente que habiliten a los titulares de datos a solicitar explicaciones ante las empresas -cuando una decisión automatizada o perfilado- le produzca efectos jurídicos negativos? En su caso, ¿los usuarios podrían solicitar la intervención de la autoridad de control de datos personales Argentina, cuando no hayan recibido respuesta de las organizaciones ante sus reclamos o se les haya contestado de manera insuficiente?

¿La actualización de la regulación será suficiente para lograr la responsabilidad proactiva en organizaciones respecto a la gestión de la información?

¿Cuál es el rol del deber de Información para el ejercicio y tutela de estos derechos?

1.3. OBJETIVOS

El presente trabajo de investigación tiene el siguiente objetivo principal:

- Describir si en Argentina existen mecanismos jurídicos en la actualidad que habiliten a los usuarios a presentar reclamos ante empresas por afectaciones en el marco de decisiones automatizadas y perfilados, y en su caso, solicitar la intervención de la autoridad de control.

Los objetivos secundarios son:

- Analizar brevemente los principales efectos de la implementación del RGPD en países desarrollados, para determinar su grado de aplicación en la práctica para el ejercicio de los derechos objeto del presente estudio.

- Reflexionar sobre la relevancia del deber de información para el ejercicio derechos y la tutela de la autoridad de control en jurisdicción nacional.

- Describir las técnicas principales de perfilados y decisiones automatizadas utilizadas en el ámbito empresarial asociadas a mercadotecnia, para lograr una visión más clara de las categorías de datos utilizadas que pueden ser objeto de reclamo por parte de usuarios o de control por la AAIP.

- Describir casos de derecho comparado, en los que se hayan registrado efectos jurídicos negativos asociados a perfilados y decisiones automatizadas, para tener una visión más específica de las afectaciones que podrían generarse en distintos contextos organizacionales.

1.4. ALCANCE

La investigación abarca únicamente su aplicación en el ámbito empresarial de servicios de tecnologías de información. El período de tiempo de recolección de la información comprende desde el año 2018 a julio de 2021.

1.5. METODOLOGÍA DE LA INVESTIGACIÓN

El presente trabajo es de tipo descriptivo, y mide las variables de interés a través de los siguientes instrumentos de recolección de la información:

- A través de la revisión de fuentes primarias de normativa internacional, nacional, directrices y buenas prácticas. Revisión de la literatura de reconocidas fuentes de normativa internacional, nacional y su conjunción, se recolectaron evidencias significativas que justifican la dimensión de la investigación. Dicho estudio permitió una descripción profunda de los mecanismos para el ejercicio de derechos en el marco del RGPD y un estudio comparativo con la normativa nacional en materia de protección de datos personales, lo que posibilitó responder las preguntas de investigación. Mediante la observación y revisión de documental, se analizaron las principales deficiencias en Políticas de Privacidad de empresas que operan en Argentina y las técnicas de marketing digital más frecuentes que emplean perfilados y decisiones automatizadas, lo que permitió obtener un análisis transversal de las posibles afectaciones generadas a usuarios en el ámbito privado.
- A través de la revisión documental de casos de derecho comparado, se logró obtener un análisis sobre los efectos del RGPD en países desarrollados vinculados con el ejercicio de derechos. Se realizó un análisis transversal de distintos casos de estudio de efectos jurídicos negativos que podrían sufrir los usuarios a través de estos tratamientos de la información en distintos contextos empresariales.

- Con entrevistas a abogados especializados en protección de datos personales, se pretendió conocer la postura sobre la posibilidad de ejercicio

de derechos en Argentina ante este tipo de procesamientos en el marco de la normativa jurídica existente.

Entrevistados:

- Horacio Granero (Presidente en el Dial.com. Ex-socio del estudio Allende & Brea)
- Melisa Sánchez (Asesora legal en privacidad en la empresa Mercado Libre)
- Facundo Malaureille (Director académico de la diplomatura de Data Governance en UCEMA)
- Diego Fernandez (Socio del área de práctica de Tecnología de la Información y Privacidad de Marval, O'Farrell & Mairal.
- Juan Pablo Altmark (Abogado, Presidente de la Asociación Latinoamericana de Privacidad (ALAP)
- Fernando Tomeo (Profesor Buenos Aires y Universidad Austral. Director del Programa Ejecutivo de Postgrado de "Derecho y Comunicación Digital"
- Hugo Vaninetti (Consultor Especializado en Tecnología y autor de diversas publicaciones en materia de privacidad y datos personales)

CAPÍTULO 2. PERFILADOS Y DECISIONES AUTOMATIZADAS EN ORGANIZACIONES

2.1. Del marketing masivo al marketing personalizado

"Cada oportunidad para interactuar con un cliente es otra oportunidad para recolectar datos",

Jeff Bezos, fundador de Amazon.

No es novedad que el marketing tradicional empleado por las organizaciones ha ido adaptando su enfoque de la mano de la evolución de las nuevas tecnologías.

En una primera etapa el marketing se caracterizó por un enfoque dirigido en forma masiva a sus clientes, por ejemplo a través de canales de televisión, radio o bien, publicidad impresa. Este esquema de llegar a los clientes ha ido mutando a una comunicación cada vez más personalizada.

En un principio, las bases de datos se analizaban con la intención de definir segmentos de clientes utilizando una variedad de métodos estadísticos para dirigirse a clientes potenciales. Por ejemplo, se tomaba un gran número de clientes y se formaban segmentos hacia un cliente "promedio", como hombres, de 18 a 24 años de edad, para en base a eso, desarrollar diferentes ofertas de productos o campañas de marketing.

Winer R. S. (2001) resalta que la revolución de la tecnología de la información y, en particular, de la World Wide Web, ofreció a las empresas la oportunidad de elegir “[c]ómo interactúan con sus clientes y establecer mejores relaciones con los clientes, lo que antes era posible en el mundo offline”. Este autor pone de resalto que, estas capacidades en línea han habilitado a las empresas mayores capacidades para establecer, alimentar y mantener relaciones con clientes a largo plazo, complementando las interacciones personales proporcionadas a través de vendedores, representantes de servicio al cliente y centros de llamadas.

Los expertos Peppers, Rogers y Dorf (1999) han instado a las organizaciones a comenzar a dialogar con sus clientes a través de enfoques específicos (“one on one

marketing"), en lugar de hablar a los clientes a través de los medios de comunicación. Argumentan que el "marketing relacional" se basa en la idea de establecer una relación de aprendizaje con cada cliente, teniendo en cuenta que los clientes de este siglo tienen menos tiempo, enfatizando que los desafíos en marketing radican en identificar sus preferencias, atraerlos con estrategias y ofrecer mensajes efectivos.

Por su parte, Kartajaya, Kotler y Hooi (2019) resaltan la transición del marketing tradicional (mercadotecnia masiva 1.0 basada en el producto y la mercadotecnia de segmentos del cliente 2.0) hacia un marketing digital 3.0, ahora centrado en el ser humano, que incluye diferentes técnicas dirigido a éste de manera personalizada. Entre los ejemplos, mencionan envíos de correo electrónico, marketing de contenidos, marketing en redes sociales, posicionamiento en buscadores que mejora la visibilidad -"SEO"-, publicidad mediante anuncios en las páginas de resultados de buscadores -"SEM"-, entre otras.

En este punto, resulta conveniente resumir brevemente algunos hitos de la publicidad virtual (Chatfield, T., 2012):

(i) un comienzo determinado por el "número de visitas" que recibía determinada página web sobre cuántas veces aparecía un anuncio a los usuarios; (ii) la aparición en el año 2000, de Google "Adwords", palabras claves que permitían a los clientes adquirir pequeños anuncios de texto en los resultados del motor de búsqueda; (iii) en el año 2002, Google introdujo en su modelo de negocios el sistema de "pago por clic" que se convirtió en su principal fuente de ingresos; (iv) en el 2003, esta misma empresa lanzó "Adsense", que permitía a cualquier propietario usar Google como su servidor publicitario; (v) La red social Twitter permite a los anunciantes que un trending topic encabece las listas o promociona cuentas corporativas; y (vi) Facebook, uno de los primeros sitios del mundo en ofrecer publicidad a los anunciantes con un targeting enormemente potente, basando su publicidad de servidor en Microsoft.

En este contexto, los autores Davenport, T. H., Barth, P., & Bean, R. (2012) ponen de relieve la principal diferencia entre las tecnología de la información (TICs) y la analítica de big data o "macrodatos", identificando a las primeras como más retrospectivas y preocupadas por supervisar los procesos y notificar la gestión de anomalías; mientras que la analítica de big data o "macrodatos", se concibe

orientada hacia el futuro, porque implica la extracción de fuentes de datos existentes para detectar nuevos patrones, eventos y oportunidades.

En conexión con lo anterior, la OCDE (2013) ha elaborado un informe en el que estudia el valor económico de los datos y su relación con los modelos de negocio, en la que se distinguen las siguientes categorías:

- Datos generados por los usuarios (incluyendo posts en redes, comentarios, fotos y vídeos);
- Datos sobre actividad o comportamentales (incluyendo qué busca y ve la gente mientras navega por Internet, qué compra online, cuánto gasta y cómo realizan el pago);
- Datos sociales (incluyendo contactos y amigos en redes sociales);
- Datos sobre ubicación (incluyendo domicilio permanente, posicionamiento y geolocalización, dirección IP)
- Datos demográficos (edad, sexo, raza, nivel de ingresos, orientación sexual, afinidad política), y
- Datos identificativos (información financiera y números de cuenta, información de salud, número de Seguridad Social, antecedentes policiales, otros).

Barforoush, A., Shirazi, H., & Emami, H. (2017) plantean que el gran volumen y "caos" de datos de la Web, trajo problemas como la sobrecarga de información, lo que generó la necesidad de crear enfoques más eficientes para transformar los datos en formato estructurado, extrayendo y conectando todo el conocimiento.

2.2. Marketing 5.0: IA, perfilados y decisiones automatizadas

A raíz de esta necesidad, como la de establecer mediciones de variables, comportamiento de los clientes y retornos de inversión en tiempo real, las herramientas de analítica han cobrado un protagonismo sin igual para todas las organizaciones.

El marketing tradicional ha evolucionado a un marketing 5.0 que emplea inteligencia artificial ("IA"): se emplean procesamientos automatizados de grandes volúmenes de

datos, se realizan predicciones y se elaboran perfiles de usuarios para ofrecerles determinados bienes y servicios, o seguimiento de diversas cuestiones.

Previo avanzar con el análisis de cuestiones normativas vinculadas a afectaciones por operaciones automatizadas, resulta necesario abordar brevemente los conceptos más básicos relativos a IA, perfilados y decisiones automatizadas.

Existen muchas definiciones que intentan conceptualizar a la IA.

Una definición práctica es la brindada por los autores Agrawal, Gans, Goldfarb, Milutinovic (2018) que parten de la analogía que "los datos son petróleo", ejemplificando que, así como los motores de combustión interna necesitan petróleo para funcionar, la IA necesita datos, ya que “[l]a IA son máquinas de predicción conducidas por datos”.

De este modo, estos autores explican que la IA utiliza datos en bruto y los convierte en algo útil para la toma de decisiones en las empresas, por ejemplo, del siguiente modo: “¿Qué tiempo hará mañana? Usemos datos sobre el tiempo del pasado. ¿Queremos saber las ventas de yogurt para la próxima semana? Usemos datos de ventas de yogurt anteriores”.

Otro aspecto al que hacen alusión, es a la relación entre el entrenamiento de la máquina y el valor constante de los datos de las acciones realizadas diariamente, dado que los nuevos datos acumulados cada día son los que permiten entrenar la IA con distintos fines.

Una tercera cuestión sobre la que hacen hincapié estos autores, consiste en el mejoramiento de la máquina de predicción mediante el aprendizaje. Puntualizan que “[s]i bien 10 años de datos sobre las ventas de yogur en el pasado son valiosos para entrenar a un modelo de Inteligencia Artificial para predecir futuras ventas de yogurt, las predicciones reales utilizadas para administrar la cadena de suministro, requieren datos operativos de forma continua”. De lo anterior, es que suele asociarse que el término IA imita funciones “cognitivas” como el aprendizaje y la solución de problemas usualmente vinculadas al ser humano.

Mientras que, por otra parte, la elaboración de perfiles, es definida como un proceso que puede basarse en la toma de decisiones automatizadas, en función de patrones o factores predeterminados. Esta información crea un perfil de la persona en cuestión, de su comportamiento y lo complementa con otra información obtenida de fuentes disponibles, como intermediarios de datos, redes sociales (incluidos los “me gusta” en publicaciones y fotos), de la música que escucha por internet, datos de GPS y rastreo (Russell, S., & Norvig, P., 2002).

Por ejemplo, los procesamientos automatizados se encuentran presente en diversos campos como por ejemplo, en traductores automáticos, el reconocimiento facial, la clasificación de correos, el asistente de voz, los mapas e indicaciones en tiempo real, los chatbots de asistencia al cliente, los contenidos y productos ofrecidos en redes sociales y/o intermediarios de Internet, hasta el teléfono celular, entre otros.

Por otra parte, la elaboración de perfiles basados en los macrodatos implica la búsqueda de patrones que reflejen “características de un tipo de personalidad”; por ejemplo, cuando las empresas publicitan productos a los usuarios como “también te pueden interesar”, basándose en información recopilada de los productos que el cliente ha comprado anteriormente o ha estado visualizando.

Según Damia, J.M., (2010) otra de las técnicas consiste en comparar los comportamientos en la web para después identificar patrones similares, construir grupos de personalidades y variables asociadas a perfiles categorizados como “Cliente de alto valor” (su valor de compra promedio es alto), “cliente generador de valor” (compre o no recomienda a otros clientes que sí lo hacen), y/o “cliente fidelizado” (sin importar el monto de su compra, hace mucho que es cliente y sigue siéndolo), entre otros.

Por lo que, las decisiones automatizadas incluyen la elaboración de perfiles, consisten en cualquier forma de evaluación automática de “aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos”.

Un ejemplo brindado por el Grupo de Trabajo del Artículo 29 del Consejo Europeo, sobre decisiones automatizadas y perfilados (2017), refiere que para valorar rápidamente la solvencia de un futuro cliente, las agencias de referencia de crédito recopilan determinados datos, sobre cómo ha mantenido el cliente sus cuentas de crédito, los detalles de los domicilios anteriores, así como información de fuentes públicas, como registros públicos (incluidas sentencias judiciales) o datos de quiebra o insolvencia. Estos datos personales se incorporan automáticamente a un algoritmo de calificación, que calcula el valor total que representa la solvencia del cliente potencial.

2.3. Mercadotecnia y técnicas de personalización

Una de las principales técnicas de la última década con fines publicitarios y orientación, ha sido la publicidad de terceros a través del Identificador de anunciantes.

Estos identificadores o ID se asocian a cada dispositivo móvil a través del sistema operativo de Iphone (IOS) o el sistema operativo de Google (Android). También son conocidos como "supercookie", ya que identifican a un dispositivo específico, y permiten a los anunciantes crear un perfil detallado de la actividad en diferentes aplicaciones o sitios web cuando ven este identificador asociando actividad con él, figurando asociados a la dirección de correo electrónico de un usuario.

Un examen llevado a cabo por Thurm, S., & Kane, Y. I. (2010) ha revelado que, de ciento un aplicaciones populares para teléfonos inteligentes:

(i) cincuenta y seis aplicaciones transmitieron la información relativa al ID, a otras empresas sin el consentimiento de los usuarios;
(ii) cuarenta y siete aplicaciones transmitieron la ubicación del teléfono; y
(iii) cinco enviaron edad, sexo y otros datos personales a personas ajenas.

Estos mecanismos no permitían el bloqueo de este tipo de publicidad en ninguno de los dos sistemas operativos mencionados, hasta el pasado 20 de marzo de 2021 que se ha dado un cambio trascendental -que podría tener implicancias para muchas empresas-.

En efecto, la empresa Apple lanzó una nueva función para su sistema operativo denominada “Transparencia de seguimiento de aplicaciones”, que permite la privacidad por diseño, en materia de anuncios para su sistema operativo IOS (Apple, 2021), evitando el seguimiento por defecto, como ha sucedido hasta el momento.

Esta nueva funcionalidad podría tener grandes impactos en la privacidad de los usuarios que utilizan iPhone, ya que ahora pueden elegir no habilitar el rastreo de sus acciones de su ID como venía sucediendo. Además, Apple advirtió que si se entera que cualquier desarrollador de aplicaciones está rastreando a los usuarios que piden no ser rastreados, les exigirá que actualicen sus prácticas para respetar la elección del usuario o bien, su aplicación será rechazada en App Store (Apple, 2021).

En cuanto al sistema operativo Android de Google, su CEO Sunder Pichai, recientemente ha referido que están trabajando en una técnica llamada “derecho de privacidad diferencial”. Ésta trataría de una tecnología que permitiría obtener conocimientos de grandes conjuntos de datos, sin obtener información de usuarios en particular de ese grupo (Iproup, 2021).

A continuación, a modo ejemplificativo se enumeran algunos de los procedimientos más frecuentes de publicidad dirigida existentes en la actualidad, además de la antes mencionada que implica la elaboración de perfilados.

Análisis de macrodatos: Tratamiento, análisis y evaluación de volúmenes de datos con el fin de obtener información útil, que pueden utilizarse con fines distintos de los previstos en un principio, por ejemplo, para obtener tendencias estadísticas o desarrollar servicios más adaptados, como la publicidad. Por ejemplo: puede evaluar transacciones financieras, solvencia, tratamiento médico, consumo privado,

actividad profesional, itinerarios utilizados, y uso de internet, para citar algunos (Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa, 2018).

Análisis de metadatos: Inferencias de otros datos que permiten extraer conclusiones precisas sobre la vida privada de las personas, como sus relaciones sociales, sus costumbres y actividades de la vida cotidiana, derivados de los sitios web visitados, localización geográfica, llamadas, contactos, entre otros (Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa (2018).

Cookies: ficheros generados por una página web y almacenados en el navegador del usuario que contienen información sobre su actividad en internet y los asistentes virtuales, capaces de escuchar constantemente las conversaciones mantenidas en su presencia y tratar todos esos datos (Rubio, 2019).

Píxel de conversión: Monitoriza el comportamiento de los usuarios que han hecho clic en una de las campañas de publicidad digital y permite saber qué páginas ha visitado, si han añadido un producto al carrito o si han finalizado el pago, entre otras acciones. Permite medir el Retorno de la inversión (ROI) y optimizar los anuncios para que sean más rentables (Apple, 2021).

Subastas de anuncios digitales: Este proceso tiene lugar en tiempo real, durante el cual distintos anunciantes pujan por el espacio publicitario ofrecido por las empresas Google (buscador) y Facebook (redes asociadas). Cuando el usuario abre la aplicación, la red publicitaria recopila datos del uso del dispositivo (por ejemplo, qué aplicación está usando, su ubicación, y el ID de publicidad). La red publicitaria comparte parte de esta información, en particular, el ID de publicidad, con anunciantes potenciales. Antes las pujas, los anunciantes tratan de aprender tanto como sea posible sobre el usuario a través de los datos recopilados y agregados mediante seguimiento y elaboración de perfiles. (Apple, 2021)

Atribución de la publicidad: Después de mostrar su anuncio al usuario, las empresas de publicidad están interesadas en medir su efecto en el comportamiento. Para ello, el anunciante trata de rastrear el comportamiento en el dispositivo, recoger información sobre lo que hace en la web, en las aplicaciones e incluso en los lugares a los que acude sin conexión. Los anunciantes también utilizan la atribución

de anuncios para "optimizar" su campaña publicitaria hacia grupos para los que la campaña publicitaria es más eficaz. (Apple, 2021)

Intermediario o “corredor” de datos: En general, es una empresa que recoge, regularmente y vende, licencia o divulga de otro modo a terceros la información personal de determinados usuarios finales con los que la empresa no tiene una relación directa (Apple, 2021)

CAPÍTULO 3. EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS PERSONALES (“RGPD)

3.1. Decisiones automatizadas y perfilados

Como ya hemos referido, la elaboración de perfiles y las decisiones automatizadas pueden resultar de utilidad para las organizaciones, dado que ofrecen beneficios como mayor eficiencia y ahorro de recursos, mejoras en la segmentación, personalización de productos y servicios, entre otras cuestiones.

En particular, el artículo 4 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (en adelante “RGPD”) define la elaboración de perfiles como “[t]oda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física”.

Asimismo, el Reglamento la define como “[i]dentificadores en línea [...], como direcciones de los protocolos de internet, identificadores de sesión en forma de “cookies” u otros identificadores, como etiquetas de identificación por radiofrecuencia [...] puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, que pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas”.

Al respecto, las Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679 (Grupo de Trabajo del artículo 29, 2017), explican que la elaboración de perfiles puede implicar tres fases distintas tales como: (i) la recogida de datos; (ii) el análisis automatizado para identificar correlaciones; y (iii) la aplicación de la correlación a una persona para identificar características de comportamientos presentes o futuros.

En otras palabras, la elaboración de perfiles está formada por los siguientes elementos: (i) una forma automatizada de tratamiento (aunque la participación humana no excluye necesariamente la actividad de la definición); (ii) debe llevarse a cabo respecto a datos personales; y (iii) su objetivo debe consistir en evaluar aspectos personales sobre una persona física.

En este punto, resulta importante hacer una distinción entre el análisis de información o clasificaciones que no implican necesariamente una elaboración de perfil, de las que sí.

Las citadas Directrices explican que por ejemplo, las estadísticas de personas basada en características como la edad o sexo con la finalidad de tener una visión global de estos, -es decir sin sacar conclusiones sobre una persona en particular-, no equivaldría a una elaboración de perfil, puesto que no tiene como finalidad la evaluación de características individuales. Por el contrario, en las mismas también se indica que, cuando las empresas proponen al usuario productos que "también te pueden interesar" basándose en información recopilada de los productos que anteriormente ha comprado, se evidencia que han buscado previamente patrones de "características de un tipo de personalidad" basado en macrodatos, asociados a la elaboración de un perfil determinado.

Otro ejemplo allí planteado es el caso de un agente de datos que ha llevado a cabo una elaboración de perfiles asignando a la persona una categoría determinada, según sus intereses e información recabada a partir de distintas fuentes para desarrollar perfiles sobre las personas, disponerlas en segmentos y vender esta información a empresas (Grupo de Trabajo del artículo 29, 2017).

De este modo, el RGPD concibe tres formas distintas de realización de elaboración de perfiles: (i) la elaboración de perfiles general; (ii) las decisiones basadas en la elaboración de perfiles (ej. el caso en el que un ser humano decide si aprueba el préstamo sobre la base de un perfil elaborado únicamente mediante tratamiento automatizado); (iii) decisiones basadas únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que producen efectos jurídicos en el interesado o le afectan significativamente (artículo 22, apartado 1 del RGPD). Este sería el

supuesto en el que un algoritmo decide si el préstamo debe aprobarse y la decisión se traslada automáticamente a la persona en cuestión, sin ninguna evaluación previa por parte de un ser humano.

Las Directrices también refieren puntualmente que “[l]os responsables pueden llevar a cabo la elaboración de perfiles y adoptar decisiones automatizadas siempre que cumplan todos los principios y dispongan de unas bases jurídicas para el tratamiento. En el caso de decisiones basadas únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, se aplican garantías y restricciones adicionales según lo definido en el artículo 22, apartado 1. (Grupo de Trabajo del artículo 29, 2017).

Asimismo, en dicho documento se plantea que las decisiones automatizadas representan la capacidad de tomar decisiones por medios tecnológicos, sin la participación del ser humano y pueden basarse en cualquier tipo de datos por ejemplo: datos ofrecidos directamente por las personas afectadas; datos observados acerca de las personas (datos de ubicación); y datos derivados o inferidos como, por ejemplo, un perfil ya existente de la persona (por ejemplo, una calificación crediticia). Este tipo de decisiones pueden solaparse parcialmente con la elaboración de perfiles o derivarse de ésta, puesto que un tratamiento que empieza como un simple proceso de decisiones automatizadas, puede convertirse en un proceso basado en la elaboración de perfiles, dependiendo del uso que se dé a los datos (Grupo de Trabajo del artículo 29, 2017).

Un ejemplo de las citadas Directrices sobre esta cuestión es la imposición de multas por exceso de velocidad que se realiza únicamente sobre la base de las pruebas de los radares de velocidad. Esta multa posteriormente podría convertirse en una decisión basada en la elaboración de perfiles si los hábitos de conducción de la persona son supervisados a lo largo del tiempo y, por ejemplo, la cuantía de la multa a imponer es el resultado de una evaluación que implique otros factores, como si el exceso de velocidad es un caso de reincidencia o bien, si el conductor ha cometido otras infracciones de tráfico recientemente. Se plantea un caso similar en el caso de un banco que antes de conceder una hipoteca tenga en cuenta la calificación crediticia del interesado.

3.2. Procesamientos automatizados

El artículo 21 del RGPD, en su inc. 2 establece que cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de sus datos personales, incluida la elaboración de perfiles.

No obstante, el artículo 22 del RGPD prohíbe todas las decisiones que afecten al interesado que se hayan basado únicamente en el procesamiento automatizado, determinando que "[t]odo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar".

Es decir que, la regla general es que, el responsable del tratamiento no debe efectuar este tipo de tratamientos automatizados, salvo las excepciones estipuladas que a continuación se analizarán, siempre y cuando los procesamientos no se basen en datos de salud o se refieran a menores.

En este caso, el usuario podría oponerse en cualquier momento (art. 21), a menos que el responsable pueda interponer una excepción que acredite motivos legítimos que prevalezcan sobre los derechos del interesado.

Las excepciones son: (i) cuando es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento; (ii) cuando se establecen medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado (ej. las alusivas a prevención de fraude, evasión fiscal y/o, garantías de seguridad en el marco del servicio prestado); y/o (iii) cuando el tratamiento está basado en el consentimiento explícito del interesado.

Se puntualiza que en los casos i) y iii), el responsable del tratamiento deberá adoptar las medidas adecuadas para salvaguardar los derechos y libertades y los intereses

legítimos del interesado, las que implicarán como mínimo el derecho del interesado a obtener intervención humana, a expresar su punto de vista y a impugnar la decisión.

Por lo que, allí se plantea que el derecho de oposición no es un derecho absoluto y que el responsable podría negarse a cumplirlo si puede demostrar motivos legítimos convincentes para su procesamiento. Para ello, se estima que el responsable de la organización merituará los intereses, derechos y libertades de la persona con sus bases legales, debiendo demostrar que sus motivos legítimos, prevalecen por sobre los invocados por el individuo. De manera posterior, la organización en cuestión tendría que explicarle al titular su decisión e informarle su derecho a presentar una queja ante la autoridad supervisora.

3.3. Excepciones al derecho de oposición

Por su relevancia en el objeto de estudio, a continuación se ahondará en las excepciones previstas al derecho de oposición.

1. Tratamiento basado en el consentimiento explícito del interesado.

En particular, el artículo 4, apartado 11, del RGPD define el consentimiento como "[t]oda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen".

En este punto, el RGPD refuerza el requisito de que el consentimiento debe ser informado, vinculado íntimamente con el principio de transparencia (artículo 5 del RGPD) y con los principios de lealtad y licitud. La transparencia así, es concebida como "ex ante", en el sentido que el controlador de datos debe informar al sujeto con anticipación que usará sus datos para la toma de decisiones o perfilados.

Por lo tanto, el sujeto tendría la posibilidad de prestar su consentimiento informado o bien, expresar su punto de vista. Este último punto, hace presuponer que el consentimiento como regla general, deberá ser granulado en el marco RGPD.

En forma adicional se dispone para que el consentimiento sea informado y válido, al menos, se debería informar: (i) identidad del responsable del tratamiento; (ii) el fin de cada una de las operaciones de tratamiento para las que se solicita el consentimiento; (iii) qué tipo de datos van a recogerse y utilizarse; (iv) la existencia del derecho a retirar el consentimiento; e (v) información sobre el uso de los datos para decisiones automatizadas de conformidad con el artículo 22, apartado 2, letra c), cuando sea pertinente.

En la misma sintonía, el deber de información (art. 13 del RGPD) establece como información adicional, informar: (i) la existencia de decisiones automatizadas, incluida la elaboración de perfiles (artículo 22, apartados 1 y 4) y, en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado; y (ii) que cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2, entre otras cuestiones.

El considerando 39 del RGPD -en cuanto al principio de transparencia en el contexto del tratamiento de datos- refiere concretamente, que "[p]ara las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados".

Por su parte, la Guía de Privacidad desde el Diseño de la Agencia Española de Protección de Datos (2019) en este punto determina concretamente que "[l]a transparencia en el tratamiento de datos se asienta como pilar para demostrar la diligencia y la responsabilidad proactiva ante la Autoridad de Control y como medida de confianza ante los sujetos cuyos datos son tratados" y que, "[t]al y como establece el considerando 39 del RGPD, para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados".

Las recomendaciones del Grupo de Trabajo del art. 29 (“GT29”) sobre las Directrices de Transparencia recomiendan, que para evitar la fatiga informativa de los usuarios, se debe facilitar como buena práctica un enlace al aviso de privacidad en el punto de recogida de los datos personales o que esta información esté disponible en la misma página en que estos se recogen.

2. Tratamiento necesario para la celebración o la ejecución de un contrato

No es novedad que a menudo, la financiación de los servicios en línea que no implican el pago de una tarifa por los usuarios, tienden a analizar el comportamiento en línea y las actividades asociadas de seguimiento y elaboración de perfiles para fines de publicidad.

Al respecto, el Dictamen del Consejo Europeo sobre las aplicaciones de los dispositivos inteligentes y publicidad del comportamiento en línea (2013) determina que los responsables del tratamiento deben recabar el consentimiento previo de los interesados para utilizar las cookies necesarias para las actividades de publicidad comportamental. Por ende, como regla general, el tratamiento de datos personales con fines de publicidad del comportamiento, no es considerado necesario para la ejecución de un contrato de servicios en línea, concediéndose a los interesados un derecho absoluto de oposición al tratamiento de sus datos con fines de mercadotecnia (artículo 21 RGPD).

En otras palabras, el referido Dictamen determina que cuando la personalización del contenido no es necesaria desde el punto de vista objetivo para los fines del contrato subyacente (por ejemplo, cuando el contenido personalizado ofrecido tenga por objeto incrementar el uso del servicio por parte del usuario, pero no forma parte esencial del uso del servicio), los responsables del tratamiento deberán utilizar una base legal alternativa a la hora de invocar una excepción.

Las citadas Directrices ejemplifican esta cuestión en el siguiente ejemplo. Una página de búsqueda de hoteles realiza un seguimiento de las reservas anteriores de los usuarios con el fin de crear un perfil de su gasto habitual. Este perfil se utiliza

posteriormente para recomendar determinados hoteles al usuario en los resultados de la búsqueda. En este caso, la elaboración del perfil con los datos financieros y del comportamiento previo del usuario no es necesaria desde el punto de vista objetivo para la ejecución del contrato; por tanto, no resultaría aplicable a esta actividad de tratamiento la excepción.

3.4. Derecho de acceso

El RGPD dispone en su artículo 15 la posibilidad que el titular del dato le consulte al responsable de tratamiento si se están tratando o no datos personales que le conciernen y, en tal caso, se habilita el derecho de acceso. Los responsables del tratamiento podrían considerar la aplicación de un mecanismo para que los interesados comprueben su perfil, incluidos detalles de la información y las fuentes utilizadas para elaborarlo.

Entre otras cosas, este derecho habilita al titular a obtener la siguiente información a través del derecho de acceso: (i) fines del tratamiento, (ii) categorías de datos, (iii) los destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales; (iv) el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo; (v) derecho a solicitar la rectificación, supresión, limitación u oposición del tratamiento; (vi) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen y (vii) el titular también tiene derecho a que se le facilite una copia de los datos personales objeto de tratamiento.

En el marco de este derecho, se estipula que los responsables deben permitir a los interesados la posibilidad de actualizar o modificar cualquier inexactitud en los datos o del perfil (art. 16).

También se habilita al titular a solicitar al responsable información sobre “[l]a existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información

significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado".

3.5. Derecho a obtener intervención humana

El citado Grupo de Trabajo expresó que para que la decisión quede sometida al artículo 22, se requiere que la intervención humana sea significativa en el sentido de que debe ser "[r]ealizada por alguien con la autoridad y competencia para cambiar la decisión"; por lo que para ello, será necesario que esta persona tenga acceso a información, más allá de los productos o resultados que arroje el algoritmo.

Por tanto, se consideró que la intervención de un Oficial de Protección de Datos ("DPO") resulta fundamental, entre otras tareas, para los siguientes propósitos: (i) para excluir la discriminación y el perfil de menores; (ii) para reducir los falsos positivos debido a correlaciones estadísticas que deben prevenirse; (iii) para fomentar la trazabilidad, y explicabilidad ante el interesado, o bien por parte de la institución de monitoreo externa (es decir, la Autoridad de Protección de Datos o en su caso, los tribunales judiciales).

3.6. Evaluaciones de impacto

El artículo 35 del RGPD, establece la obligación de implementar la protección de datos desde el diseño a todos los responsables del tratamiento, mediante la aplicación de medidas técnicas y organizativas apropiadas "[t]anto en el momento de determinar los medios de tratamiento, como en el propio tratamiento".

Si bien el cumplimiento de esta obligación aplica específicamente al responsable del tratamiento, se aclara que la protección de datos desde el diseño se concibe proyectada sobre otros actores participantes en el tratamiento de datos personales, de manera transversal a toda la organización.

El enfoque de la privacidad basado en el riesgo (artículo 35) introduce la obligación del responsable de realizar una evaluación de impacto antes de proceder a un

tratamiento cuando sea probable que éste entrañe “un alto riesgo” para los derechos y libertades de las personas físicas (es decir, no resulta obligatorio en todas las operaciones de tratamiento).

Conforme surge de las Directrices sobre la evaluación de impacto relativa a la protección de datos para determinar si el tratamiento “entraña probablemente un alto riesgo” (Europea U., 2017), un “alto riesgo” tendría lugar cuando el responsable del tratamiento no pueda hallar suficientes medidas para reducir los riesgos hasta un nivel aceptable (es decir, los riesgos residuales siguen siendo elevados), razón por la cual, la organización deberá consultar a la autoridad de control en materia de privacidad.

En particular, las Directrices disponen que el tratamiento automatizado y la elaboración de perfiles, exigirán la realización de una evaluación de impacto, dado que éstas deberán realizarse en el caso que se realice una “[e]valuación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar”.

Esta evaluación deberá incluir como mínimo: (i) una descripción sistemática de las operaciones de tratamiento previstas y fines legítimos que habilitan el tratamiento; (ii) una evaluación de la necesidad y proporcionalidad con respecto a su finalidad; (iii) una evaluación de los riesgos para los derechos y libertades de los interesados; y d) medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos para proteger los derechos de los titulares (Europea U., 2017),

Las Orientaciones Específicas para la Aplicación de Medidas Proactivas en el Tratamiento de los Datos Personales de los Proyectos de Inteligencia Artificial (IA) emitidas por la Red Iberoamericana de Protección de Datos (2019), resaltan la importancia de medidas consistentes en:

(i) “[e]mbeber la privacidad como requisito en el diseño y la arquitectura del programa, servicio, sistema, plataforma o cualquier otra tecnología de IA, con el objetivo de proponer medidas técnicas para los riesgos de privacidad identificados antes de que éstos se materialicen”;
(ii) que “[los desarrolladores de IA adapten la lógica de los algoritmos, de modo que los sistemas de IA permitan garantizar por defecto, la seguridad de los datos personales y así dar cumplimiento a las obligaciones en la materia”; y
(iii) documenten “[l]as evaluaciones de impacto a la privacidad que se realicen, para que, en un momento específico, puedan presentarse a la Autoridad de Control o Autoridad de Protección de Datos competente, en el caso de una inspección o si surge una controversia al respecto”.

Tal como se establece en las Directrices del GT29 sobre la evaluación de impacto (Europea U., 2017), los responsables del tratamiento podrían considerar la publicación de dicha evaluación (o una parte de ella), como forma de reforzar la confianza en las operaciones de tratamiento, demostrar transparencia y responsabilidad proactiva.

Asimismo, el cumplimiento de un código de conducta (previsto en el artículo 40) puede contribuir a demostrar transparencia, ya que podrían elaborarse códigos que especifiquen la aplicación del RGPD en lo que respecta al tratamiento leal y transparente de información.

3.7. Supervisión

Roig, A. (2020) considera que tanto la supervisión interna como externa es necesaria para ayudar con la implementación del art. 22 del RGPD.

De este modo, hace hincapié en que el procedimiento de supervisión interna en las organizaciones debe estar a cargo de un Oficial de Protección de Datos Personales (DPO), experto a cargo en las organizaciones de las salvaguardas en la organización, el que tiene a cargo entre sus funciones:

- garantizar el cumplimiento del art. 22;

- asegurar que se mantenga un registro de transmisión y recepción de datos personales; y
- asegurar que los interesados sean informados de sus derechos

Las Directrices detallan algunas recomendaciones que los responsables del tratamiento deberían considerar a la hora de tomar decisiones basadas únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, tales como:

- controles periódicos de aseguramiento de la calidad de sus sistemas para garantizar que las personas reciben un trato justo y no discriminatorio, tanto sobre la base de categorías especiales de datos personales, como de otra clase;
- auditorías algorítmicas: comprobación de los algoritmos utilizados y desarrollados por los sistemas de aprendizaje automático para demostrar que funcionan según lo previsto, y que no producen resultados discriminatorios, erróneos o injustificados;
- auditorías independientes de terceros;
- medidas específicas para la minimización de datos para incorporar claros periodos de conservación para perfiles y datos personales utilizados al crear o aplicar los perfiles;
- utilización de técnicas de anonimización y seudoanonimización en el contexto de la elaboración de perfiles;
- formas de permitir al interesado expresar su punto de vista e impugnar la decisión;
- un mecanismo para la intervención humana en determinados casos, por ejemplo, ofrecer un enlace a un procedimiento de recurso en el momento en que se informe al interesado de la decisión automatizada, con plazos acordados para su revisión y un punto de contacto designado para cualquier consulta; y
- Comités de ética para evaluar los daños y beneficios potenciales para la sociedad de aplicaciones concretas de la elaboración de perfiles.

En cuanto a la supervisión externa, ésta se concibe principalmente a través de las autoridades nacionales de Protección de Datos (DPA), las que tienen un papel

fundamental para evaluar “a posteriori” los criterios adoptados por las organizaciones, siendo la trazabilidad clave para una supervisión eficiente.

Respecto a la consulta previa que el responsable de tratamiento debe hacer a la autoridad de control -en el caso que una Evaluación de impacto determine que existe un nivel de riesgo residual para los derechos y libertades de los ciudadanos que podría resultar inaceptable-, el apartado 3 del artículo 36 del RGPDP enumera la documentación obligatoria a remitir a la Autoridad.

Al respecto, la Guía de Evaluación de Impacto de la Agencia Española de Protección de Datos Personales (2021) aclara que, solicitar a la Autoridad de Control la evaluación de la licitud de un tratamiento no puede implicar por ejemplo, trasladarle a la Autoridad la obligación del responsable de llevar a cabo la evaluación de la proporcionalidad y/o necesidad del tratamiento, como así tampoco, la validación de la Evaluación o la identificación de los riesgos.

En efecto, el artículo 57.1 establece que incumbirá a cada Autoridad de Control, en su territorio, “[o]frecer asesoramiento sobre las operaciones de tratamiento contempladas en el artículo 36, apartado 2”.

Es decir que, el asesoramiento de la Autoridad de Control podrá incluir alguno de los siguientes aspectos: (i) señalar al responsable que el tratamiento podría infringir el RGPD, (ii) determinar si el tratamiento puede ejecutarse en las condiciones de riesgo descritas por el responsable, e (iii) informar al responsable la adecuación de las medidas para evitar los riesgos del tratamiento para los derechos y libertades.

En el apartado segundo del artículo 36 se establece además que, ante la información remitida por el responsable, la Autoridad de Control también podrá extender su acción a la totalidad de los poderes de investigación (artículo 58.1) y poderes correctivos (artículo 58.2) pudiendo requerir al responsable, información adicional y/o realizar investigaciones en forma de auditorías que podrían incluir el acceso a los locales, equipos, datos y la información necesaria para el ejercicio de las funciones de control.

3.8. Reflexiones sobre las dificultades normativas del RGPD

En primer lugar, cabe mencionar que la Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa (2018), advierte como dificultad la naturaleza de los procesamientos automatizados que, de por sí, para su funcionamiento, ya se requiere de un gran volumen de datos para el entrenamiento de las predicciones, los que en general exceden el ámbito de finalidad inicial y los plazos de conservación. En síntesis, ponen de relieve que este tipo de procesamientos tienden a contrariar precisamente el espíritu de los principios generales de protección de datos (minimización de datos, calidad, finalidad, conservación, consentimiento, otros).

En segundo lugar, en cuanto a la explicabilidad de este tipo de procesamientos, Goodman, B. & Flaxman, S. (2017) advierten que el Reglamento carece de un lenguaje preciso y presenta un vacío legal sobre algunas cuestiones, lo que presenta el riesgo de convertirlo en ineficaz.

Por ejemplo, resaltan que (i) existe incertidumbre sobre si el uso de procesos automatizados para la preparación de una decisión constituye únicamente procesos automatizados, es decir si el ser humano que toma la decisión final no desea interferir o adoptar la decisión; (ii) que tampoco se aclara si la "explicación" hace referencia a la funcionalidad del sistema (la lógica, la importancia, las consecuencias previstas y la funcionalidad general de un sistema de toma de decisiones automatizado, por ejemplo, la especificación de requisitos del sistema, árboles de decisión, modelos predefinidos, criterios y estructuras de clasificación); o bien, a las decisiones específicas (la justificación, las razones y las circunstancias individuales de una decisión automatizada especifica, la ponderación de características, reglas de decisión específicas de caso definidas por máquina, información sobre grupos de referencia o perfiles); y que (iii) tampoco se aclara qué cuenta como un efecto legal significativo de la decisión automatizada, incluida la elaboración de perfiles.

En particular, Edwards, L., & Veale, M. (2017) ha sugerido que las personas sujetas a la toma de decisiones algorítmicas deben recibir tanto lo que ellos llaman explicaciones "centradas en el modelo" y "centradas en el sujeto". Las primeras

deberían incluir: la familia del modelo, los datos de entrada, las métricas de rendimiento y cómo se probó un modelo. Mientras que las centradas en el sujeto deberían incluir contrafactuales (es decir, qué cambios se podrían realizar sobre el resultado de una decisión individual), las características de individuos clasificados de manera similar y la confianza que un sistema tiene en un resultado.

En concordancia, Kartajaya, H., Kotler, P., & Hooi, D. H. (2019) ponen de relieve que el enfoque actual en el derecho a la explicación es demasiado estrecho y piden a los controladores de datos que utilicen conscientemente el proceso de evaluaciones de impacto obligatorios para producir lo que llaman "explicaciones multicapa" de los sistemas algorítmicos.

Estos autores resaltan la importancia de (i) un Modelo de Evaluación de Impacto Algorítmico que sea verdaderamente continuo; (ii) la publicación de la evaluación de impacto -al menos en forma de resúmenes significativos-, basado en la creencia que esto ayudará a abordar las preocupaciones sobre la falta de participación de las partes interesadas; y (iii) la supervisión regulatoria sobre el proceso de evaluación de impacto a través de inspecciones a empresas para verificar su cumplimiento y/o establecer prácticas más concretas y específicas acordes al sector en torno a la equidad algorítmica.

Por el contrario, Roig, A. (2020) advierte que la supervisión en tiempo real parece imposible e innecesariamente complicada, enfatizando que se debe “[e]vitar la revisión externa a ciegas del procesamiento automatizado sólo en base al principio de proporcionalidad o razonabilidad”. Refiere que esto podría ocurrir cuando “[u]n tribunal, una autoridad de protección de datos (DPA) u otra autoridad, -sin información relevante sobre la toma de decisiones monitoreada-, decida si el resultado es proporcionado o razonable, y se pregunta “¿Cómo puede un juez evaluar la necesidad o adecuación de un procesamiento sin monitorear de cerca el proceso interno?”.

Este autor destaca que (i) para que la revisión externa sea efectiva, ésta debe darse en forma conjunta con la supervisión interna (es decir, con la organización en particular) debiendo modelarse juntas; (ii) resalta el rol del monitoreo latente y el

empoderamiento de los tribunales y de las autoridades de datos externas de supervisión; y (iii) la interdisciplinariedad como condición indispensable para la aplicación exitosa del RGPD, concluyendo que “[s]i los abogados continúan pasando por alto los aspectos técnicos de la regulación, no sólo el art. 22 del RGPD no se implementará adecuadamente, sino que los derechos de los interesados también estarán en riesgo”.

En similar sentido, Metcalf, J., & Crawford, K. (2016) si bien elogian los esfuerzos del RGPD como un buen comienzo, se centran en las deficiencias existentes de las evaluaciones de impacto, refiriendo que ésta consiste solo en una medida indirecta del daño subyacente y que será difícil que no se conviertan solo en un documento en el que se marcan casillas. Enfatizan que, si bien la rendición de cuentas es necesaria, estas evaluaciones no necesariamente medirán los daños, ya que también éstos podrían ser ocultados por las organizaciones.

Alsimismo, los citados autores refieren que describir daños reales que incluyen aspectos sociales y psicológicos de la humanidad, resulta extremadamente complejo de evaluar y mucho menos de cuantificar. Ponen como ejemplo que si bien una Evaluación podría medir hasta qué punto su modelo de reconocimiento facial se desvía de su punto de referencia de equidad (basado en una política de la empresa) de que los resultados del modelo, esta métrica no medirá el daño emocional o psicológico causado a los individuos y mucho menos a comunidades enteras, cuando el algoritmo los reconoce erróneamente repetidamente. Tampoco, captará los daños más fácilmente cuantificables como una pérdida económica que puede derivarse de estos sistemas sesgados.

Otro aspecto que cuestionan es que al hacer una evaluación de impacto resultará difícil evaluar su exhaustividad porque no existe un estándar objetivo con el que medir. “¿Cuándo sabe una empresa que ha evaluado adecuadamente todos los impactos que podrían enfrentar sus clientes y otras partes interesadas indirectas de su producto?” También advierten que, la idoneidad de los Algoritmos se juzga actualmente por lo que los autores denominan "comunidades epistémicas" o el consenso de expertos que se encuentran en la mesa, subrayando que no será representativo de todas las voces en la prevención de daños (Metcalf, et al, 2016)

Por último, respecto a la reparación del daño, el Libro Blanco sobre la inteligencia artificial (2020) plantea que la opacidad de la IA hace difícil detectar y demostrar los posibles incumplimientos de la legislación, especialmente las disposiciones legales que protegen los derechos fundamentales, imputan responsabilidades y permiten reclamar una indemnización.

CAPÍTULO 4. NORMATIVA VIGENTE EN ARGENTINA

4.1. Derecho a no ser objeto de una decisión automatizada

En la actualidad, el artículo 1 de la Ley 25.326 protege el honor y la intimidad determina que [l]a presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamietno de datos, sean éstos públicos o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad con el artículo 43, párrafo tercero de la Constitución Nacional".

El artículo 3 define a los datos informatizados como "[l]os datos personales sometidos al tratamiento o procesamiento electrónico o automatizado".

El derecho a no ser objeto de una decisión automatizada se encuentra expresamente receptado en el art. 20 de la Ley Nº 25.326, aunque limitado a decisiones judiciales y a actos administrativos que impliquen una valoración de conductas humana, determinando que "[l]as decisiones judiciales o los actos administrativos que impliquen apreciación o valoración de conductas humanas, no podrán tener como único fundamento el resultado del tratamiento informatizado de datos personales que suministren una definición del perfil o personalidad del interesado. Los actos que resulten contrarios a la disposición precedente serán insanablemente nulos".

En particular, la Resolución 4/2019 dictada por la AAIP en uso de las facultades conferidas por el artículo 29, inciso 1, apartados b) de la Ley N° 25.326, en su

artículo 1 establece la aprobación de criterios orientadores e indicadores de mejores prácticas en la aplicación de la Ley Nº 25.326, explicitando en sus considerandos que los mismos son “[d]e observancia obligatoria para todos aquellos sujetos alcanzados por la Ley Nº 25.326”. De lo anterior, se desprende como vinculante esta resolución.

El Criterio 2 de la mentada normativa determina que “[e]n caso que el responsable de la base de datos tome decisiones basadas únicamente en el tratamiento automatizado de datos que le produzcan al titular de los datos efectos jurídicos perniciosos o lo afecten significativamente de forma negativa, el titular de los datos tendrá derecho a solicitar al responsable de la base de datos, una explicación sobre la lógica aplicada en aquella decisión, de conformidad con el artículo 15, inciso 1 de la Ley Nº 25.326”. Por su parte, este artículo refiere que “[l]a información debe ser suministrada en forma clara, exenta de codificaciones y en su caso, acompañada de una explicación, en lenguaje accesible al conocimiento medio de la población, de los términos que se utilicen”.

Es dable destacar que, esta misma Resolución también contempla la posibilidad que los usuarios presenten una solicitud de derecho de acceso a sus datos personales que sean recolectados de manera automatizada, concretamente mediante sistemas de videovigilancia.

El Proyecto de ley sobre estas cuestiones prevé que, se deberá revelar la existencia de decisiones automatizadas, incluida la elaboración de perfiles con información significativa sobre la lógica aplicada. Contempla el derecho del titular a oponerse a ser objeto de una decisión basada únicamente en el tratamiento automatizado de datos, incluida la elaboración de perfiles, que le produzca efectos jurídicos perniciosos o lo afecte significativamente de forma negativa, coincidiendo en las tres excepciones a la regla general dispuestas en el RGPD (es decir, una base legal contractual, y/o autorización por ley; y/o consentimiento expreso).

Se observa que la diferencia sustancial entre ambas normativas está dada por el hecho que la normativa argentina dispone como regla general que el titular podrá oponerse a una decisión automatizada sólo cuando ésta lo afecte significativamente

de forma negativa; en lugar de estar prohibida como regla general tal como lo dispone el RGPD.

De lo anterior, podría interpretarse que este derecho está contemplado de manera "reactiva" o "a posteriori" por parte de los titulares de datos, o bien de la autoridad de control.

4.2. Deber de información

El derecho de Información se encuentra normado en el art. 6 de la Ley 25.326, que determina que "[c]uando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara:

(i) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios; (ii) La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable; (iii) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente [categorías de datos especiales y datos sensibles]; (iv) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos; y (v) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos".

En forma complementaria, la Resolución 14/2018 aclara concretamente que, todos los responsables de tratamiento "[d]eberán exhibir en forma clara y expresa en un sitio visible la información que impone el art. 6 de la Ley 25.326" (art. 2). Se estipula que además, junto esa información, se deberá acompañar el siguiente texto "[l]a Agencia de Acceso a la Información Pública, en su carácter de órgano de control de la Ley 25.326 tiene la atribución de atender las denuncias y reclamos que interpongan quienes resulten afectado en sus derechos por incumplimientos de las normas vigentes en materia de protección de datos personales" (art. 3).

Por su parte, el artículo 4 del Decreto 1558/01 establece en coherencia con el Principio de transparencia que "[p]ara determinar la lealtad y buena fe en la

obtención de los datos personales, así como el destino que a ellos se asigne, se deberá analizar el procedimiento efectuado para la recolección y, en particular, la información que se haya proporcionado al titular de los datos de acuerdo con el artículo 6º de la Ley Nº 25.326".

El Proyecto de Ley, garantiza mediante el art. 15 estos derechos del mismo modo que el actual, sólo que adicionando y unificando el contenido de la Resolución 14 en un mismo artículo.

Como novedad, el artículo 5 titulado "Principio de licitud, lealtad y transparencia" establece que los datos personales deben ser tratados de manera lícita, leal y transparente y que "[e]l tratamiento se considera leal cuando el responsable se abstenga de tratar los datos personales a través de medios engañosos o fraudulentos".

Teniendo en cuenta que la normativa nacional, así como su proyecto de ley, ponen en cabeza del usuario el derecho de oposición a los tratamientos automatizados que le generen un daño, se subraya la extrema necesidad que las organizaciones den cabal cumplimiento al Principio de Información, comunicando a los titulares de datos en sus Políticas de Privacidad si realizan este tipo de operaciones automatizadas, qué tipos de categorías de datos implementan, y demás información de la manera exigida en el RGPD.

En conexión con este punto, se advierte que será clave que dichas Políticas incorporen un mecanismo eficiente y accesible para que los usuarios puedan presentar la oposición a dichos procesamientos.

4.3. Derecho de oposición

La Ley Nº 25.326 le otorga el derecho al titular de los datos a solicitar en cualquier momento el retiro o bloqueo de su nombre de los bases de datos con fines de publicidad (lo que en la terminología del RGPD sería el "derecho de oposición").

No obstante, cabe hacer algunas aclaraciones y distinciones.

En primer lugar que, si bien la Ley Nacional de Protección de Datos Personales 25.326 contempla como principio de licitud general la necesidad de un consentimiento libre, previo e informado (art. 5), el tratamiento de datos con fines de publicidad no posee la necesidad de consentimiento previo, aunque sí se prevé la posibilidad de retiro, bloqueo, y/o derecho de acceso en cualquier momento.

En particular, el artículo 25 de la mentada normativa establece que "[s]e podrán tratar datos con fines de publicidad sin el consentimiento de su titular, cuando estén destinados a la formación de perfiles determinados, que categoricen preferencias y comportamientos similares de las personas, siempre que los titulares de los datos sólo se identifiquen por su pertenencia a tales grupos genéricos, con más los datos individuales estrictamente necesarios para formular la oferta a los destinatarios".

En forma complementaria, se determina que "[e]n la recopilación de domicilios, reparto de documentos, publicidad o venta directa y otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento".

Por su parte, el Decreto reglamentario Nº 1558/01 determina que "[e]n toda comunicación con fines de publicidad que se realice por correo, teléfono, correo electrónico, Internet u otro medio a distancia a conocer, se deberá indicar, en forma expresa y destacada, la posibilidad del titular del dato de solicitar el retiro o bloqueo, total o parcial, de su nombre de la base de datos. A pedido del interesado, se deberá informar el nombre del responsable o usuario del banco de datos que proveyó la información".

La Disposición Nº 4/2009 ha interpretado el alcance del artículo 27 de la Ley Nº 25.326 y el Decreto Nº 1558/01, aclarando que la opción para el ejercicio del derecho de retiro o bloqueo contemplada en el artículo 27, inciso 3 de la Ley Nº 25.326, debe aparecer en "[toda comunicación que se efectúe con fines publicitarios, junto con el mecanismo previsto para su ejercicio, que cuente con suficiente capacidad operativa para responder al eventual ejercicio de tal derecho".

Cabe referir también a la Ley 26.951 referida al Registro No Llame, sancionada en julio de 2014 con el objeto de "[p]roteger a los titulares o usuarios autorizados de los servicios de telefonía, en cualquiera de sus modalidades, de los abusos del procedimiento de contacto, publicidad, oferta, venta y regalo de bienes o servicios no solicitados". Entre las excepciones a la misma, se estipulan cuestiones de emergencia de interés general, cuando haya mediado el consentimiento del usuario o bien, cuando exista una relación contractual vigente "[s]iempre que se refieran al objeto estricto del vínculo y sean realizadas en forma y horario razonables y de acuerdo a la reglamentación".

En esta instancia, es conveniente señalar que, en el marco del debate público realizado durante la elaboración del primer Proyecto de Ley (2018) llevada a cabo por la Dirección Nacional de Protección de Datos Personales, sobre el tratamiento con fines de publicidad, algunos actores han criticado: (i) que la Ley 26.951 debería estar receptada dentro del art. 27 de la Ley 25.326; (ii) que el criterio que regula las bases con fines de publicidades es demasiado amplio y otorga demasiadas libertades a las empresas que hacen uso de los datos con fines publicitarios, dejando de lado los criterios y principios generales establecidos en la ley.

Ahora bien, el actual Proyecto de Ley (2020) recepta el tratamiento de datos en bases destinadas a la publicidad y el derecho de oposición (Artículo 61) de similar modo que la actual normativa (es decir, no resulta necesario el consentimiento de los titulares de los datos en forma previa). Asimismo, faculta al interesado el derecho a oponerse al tratamiento de sus datos y el responsable podría denegar este pedido en caso que existan motivos legítimos que prevalezcan sobre los derechos del titular de los datos.

Se advierte entonces que, el RGPD se diferencia del proyecto de ley argentino porque el primero como regla general prohíbe el tratamiento automatizado disponiendo ciertas excepciones; mientras que el proyecto nacional contempla como regla general el tratamiento sin consentimiento del titular, pudiendo en su caso éste oponerse o bien, interponer un reclamo ante la autoridad de control.

Otro punto relevante radica en el mecanismo que se dispondrá en la práctica para su ejercicio por los interesados para el caso de tratamientos automatizados.

Es decir, el derecho de oposición vigente de la Ley 25.326 y su Decreto reglamentario estipulan concretamente que se debe prever un mecanismo para su ejercicio -"que cuente con suficiente capacidad operativa"-, lo que lleva a la conclusión que las organizaciones que realicen operaciones automatizadas, tendrían que incorporar un mecanismo del estilo, que sea accesible para la oposición de los interesados, desde las mismas aplicaciones donde prestan sus servicios, o bien en sus Políticas de Privacidad, como por ejemplo, a través de un link que habilite fácilmente el pedido de bloqueo de los usuarios a este tipo de procesamientos.

De lo contrario, este derecho podrá ser ejercido a través de la presentación de un reclamo previo de bloqueo o "supresión" a dichos procesamientos. Esta alternativa además de ser menos práctica, en muchos casos resulta compleja porque muchas empresas ni siquiera informan sus datos de contacto para recibir este tipo de reclamos o consultas.

4.4. Derecho de acceso

El derecho a la explicabilidad tal como determina la Resolución Nro 4/2019 AAIP, podría ser ejercido por su titular a través de la presentación de una solicitud de derecho de acceso, de conformidad con el art. 14 de la Ley 25.326, presentada ante el responsable de tratamiento. De este pedido, también se infiere que se podrá

obtener el derecho a la intervención humana, en relación a dicha explicación y trazabilidad.

En el marco de dicho artículo, la organización como responsable debería proporcionar la información solicitada dentro de los diez días corridos de haber sido intimada fehacientemente por el usuario y vencido el plazo sin que se satisfaga este pedido, o si el informe fuese insuficiente, quedará expedita la acción de protección de los datos personales o de hábeas data, y la posibilidad de interponer una denuncia ante la Agencia de Acceso a la Información Pública (AAIP).

En el caso que se brinde respuesta al usuario, el art. 15 dispone que este acceso deberá comprender "la totalidad de la información perteneciente al interesado", provista de forma clara, y si fuera necesario, acompañada de una explicación en lenguaje accesible al conocimiento medio de la población. Asimismo, establece explícitamente que "[l] información debe ser amplia y versar sobre la totalidad del registro perteneciente al titular, aun cuando el requerimiento sólo comprenda un aspecto de los datos personales".

De lo anterior, si bien restarían criterios clarificadores, podría interpretarse que este artículo de la normativa vigente argentina permite hacer una interpretación en el mismo sentido que lo determina el RGPD, en cuanto a la información que el responsable debe suministrar al interesado ante un pedido de acceso sobre los procesamientos automatizados.

Por su parte, el Decreto 1558/01 agrega que el derecho de acceso permitirá al titular "[a]cceder a información sobre las fuentes y los medios a través de los cuales se obtuvieron sus datos, así como conocer las finalidades para las que se recabaron, el destino previsto para los datos personales, y conocer si el archivo está registrado conforme a las exigencias de la Ley Nº 25.326".

El Proyecto de Ley adiciona como novedad que el pedido de acceso pueda contener la siguiente información la "[o]bligación de informar al interesado sobre la existencia de decisiones automatizadas y sobre la lógica en ellas aplicada, incluida

la elaboración de perfiles, sin que ello afecte derechos intelectuales del responsable del tratamiento" (artículo 28, inciso h)

Por último, en conexión al derecho de acceso y la posibilidad del afectado de formular un reclamo, cabe hacer una breve alusión al derecho de limitación, del art. 18 del RGPD.

En pocas palabras, este habilita al usuario a oponerse a la supresión de sus datos personales que están en cabeza del responsable por si los necesitara para la "[f]ormulación, el ejercicio o la defensa de reclamaciones". Un caso práctico sería cuando el titular previamente se opuso al tratamiento en virtud del art. 21, y se está verificando si los motivos legítimos del responsable prevalecen sobre los del interesado.

Si bien este derecho no se encuentra explícitamente receptado en la normativa nacional (sí lo está en el Proyecto de Ley), consideramos de modo alguno se encuentra garantizado mediante el art. 17, inc 3 de la Ley 25.326, el que como una de las excepciones a la supresión, refiere que el responsable "[d]eberá brindar acceso a los registros en cuestión en la oportunidad en que el afectado tenga que ejercer su derecho de defensa".

Sin dudas, el derecho de acceso y el de limitación implicarán serios desafíos de responsabilidad proactiva por parte de las organizaciones, puesto que la entrega de esta información estará directamente asociada a la posibilidad de los afectados a interponer reclamos, lo que permite presumir que en muchos casos esta información no será lo suficientemente amplia como dispone la normativa.

4.5. Derecho de rectificación, actualización y supresión

La actual Ley 25.326 regula el derecho de rectificación, actualización o supresión en su art. 16. A tales efectos, se considera que la corrección o impugnación de un procesamiento automatizado, podría ser planteado por el interesado a través del

derecho de rectificación, o en su caso el derecho de supresión, el que debería ser contestado por el responsable del tratamiento en el plazo de cinco días.
En su respuesta, el responsable podría interponer algunas de las excepciones previstas que ya hemos analizado en los apartados anteriores. No obstante, se plantean interrogantes sobre algunas excepciones.

En este caso, por ejemplo, si un usuario solicita la rectificación o la supresión de un perfilado, y una organización le comunica al usuario que no procederá a la supresión porque posee una "obligación legal de conservar los datos para hacer perfilados", será importante la intervención de la AAIP para merituar estas excepciones, dado que en principio, son muy pocos los supuestos de obligaciones legales asociadas a perfilados al momento.

Lo mismo ocurrirá en el caso que la organización invoque obligaciones contractuales, dado que éstos serán supuestos serán mucho más acotados a lo que son en la actualidad.

Sobre este punto, será fundamental la mayor concientización de los usuarios en el ejercicio de sus derechos, así como su contacto con la autoridad de control para consultas, en relación a las excepciones que puedan interponer las organizaciones.

El pedido de asistencia a la autoridad de datos nacional será determinante puesto que muchos titulares ante el desconocimiento de la normativa, podrán tomar como válidas respuestas sobre excepciones a la regla en relación a sus pedidos de supresión, cuando muchas veces estas excepciones no corresponden con las bases legales invocadas.

Cabe mencionar brevemente a un precedente nacional vinculado a estas problemáticas, en el marco de la Resolución AAIP 32/2021.

Este caso se originó a raíz de una denuncia interpuesta por un usuario ante la empresa de delivery RAPPI SAS, mediante la cual solicitó la baja del servicio y la supresión de sus datos. No obstante ello, el denunciante continuaba recibiendo

publicidad no deseada en su celular. Habiendo transcurrido el plazo estipulado por la normativa, el denunciante presentó un reclamo ante la AAIP. En resumidas cuentas, la empresa contestó argumentando que no había procedido a la supresión requerida, invocando la excepción de necesidad contractual, cuando ésta no procedía porque precisamente el titular había requerido la "baja" del servicio por lo que, no estaba vigente la relación contractual. Posteriormente, la empresa invocó la excepción de obligación legal vinculada a la conservación de libros contables, lo que también la AAIP consideró que consistía en una excepción inadmisible dado que no guardaba relación con el tratamiento de datos objeto de análisis. Por último, se evidenció una conservación de datos excesiva y una falta al deber de información en sus Políticas de Privacidad. Por los motivos antes expuestos, la empresa ha sido sancionada.

4.6. Responsabilidad Proactiva y Delegado de Protección de Datos

El RGPD incorpora el principio de Responsabilidad demostrada ("accountability") y la figura del Delegado de Protección de Datos Personales (en adelante, "DPO"), para facilitar su cumplimiento.

Sin perjuicio que la Ley Nº 25.326 no introduce expresamente el principio de responsabilidad proactiva, ni la figura del Delegado de Protección de Datos Personales, la Resolución 40/2018 de la AAIP recomienda a los organismos estatales la designación de un agente de planta permanente como "[d]elegado de protección de datos personales", a fin de que cumpla la tarea de acompañar la implementación y control de cumplimiento de la política de protección de datos personales que se diseñe.

Asimismo, la Ley 25.326 prescribe explícitamente que el responsable o encargado del tratamiento, debe "[a]doptar las medidas técnicas y organizativas apropiadas a fin de garantizar un tratamiento adecuado de los datos personales y el cumplimiento de las obligaciones dispuestas por la ley y que le permitan demostrar a la autoridad de control su efectiva implementación".

En su artículo 29 inc. e), la citada Ley establece la facultad de la autoridad de control de "[s]olicitar información a las entidades públicas y privadas, las que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos personales que se le requieran [...]".

Un ejemplo de las medidas que debe adoptar el responsable del tratamiento para garantizar el cumplimiento de la Ley Nº 25.326 es la obligación de adoptar las medidas de seguridad apropiadas. En este sentido, el art. 9 dispone que "[e]l responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado".

En forma complementaria, el Decreto reglamentario (artículo 9) determina que la DNPDP "[p]romoverá la cooperación entre sectores públicos y privados para la elaboración e implantación de medidas, prácticas y procedimientos que susciten la confianza en los sistemas de información, así como en sus modalidades de provisión y utilización".

El Proyecto de actualización de la Ley 25.326 -en adelante, "Proyecto de Ley (2018)-", estipula en su artículo 43 la figura del Delegado de Protección de Datos en forma obligatoria cuando: (i) revistan el carácter de autoridades u organismos públicos; (ii) se realice tratamiento de datos sensibles como parte de la actividad principal del responsable o encargado del tratamiento; y/o (iii) se realice tratamiento de datos a gran escala.

Entre las funciones del Delegado se mencionan las de "[c]ooperar y actuar como referente ante la autoridad de control para cualquier consulta sobre el tratamiento de datos efectuado por el responsable o encargado del tratamiento". También se determina que [u]n grupo económico puede nombrar un único Delegado de Protección de Datos siempre que esté en contacto permanente con cada establecimiento.

Cabe mencionar que en el marco de la ronda de consultas públicas en el marco del Proyecto de Ley (2017), se decidió “[p]ermitir a las organizaciones decidir libremente si su autoridad encuadra o no en esta obligación, y eventualmente que la autoridad de control pueda exigir a las organizaciones demostrar el criterio aplicado para decidir sobre la designación del DPO” (Segura, P. (2021).

Por otra parte, la Red Iberoamericana de Protección de Datos (RIPD), de la que la Agencia de Acceso a la Información Pública (AAIP) forma parte junto con otros países de la región, ha aprobado ciertos estándares de protección de datos personales, los que tal como señala Peruzotti (2021), si bien no son vinculantes, podrían ser tenidos en consideración por las autoridades a la hora de merituar sanciones. Allí se establecen explícitamente los principios actualizados al RGPD. En particular, su art 37 establece explícitamente las medidas proactivas de protección (privacidad por diseño y por defecto, mecanismos de autorregulación, oficial de protección de datos personales, entre otros).

4.7. Evaluaciones de impacto

La Agencia de Acceso a la Información Pública de Argentina y Autoridad Reguladora de Uruguay (2020) junto con la autoridad de datos de Uruguay, han publicado una Guía de “Evaluación de Impacto en la Protección de Datos” (EIPD), en línea con los preceptos que hacen a las Evaluaciones de Impacto dispuestas en el RGPD.

En esta Guía de Evaluación se describen los enfoques de riesgo como la “Privacidad por diseño” y la “Privacidad por defecto”. Del mismo modo, se contempla la figura de un Responsable de datos dentro de la organización y su trabajo en conjunto con equipos multidisciplinarios a lo largo de las fases de la información a proteger.

Asimismo, la Disposición DNPDP Nº 18/2015 contempla una Guía de Buenas Prácticas en Privacidad para el Desarrollo de Aplicaciones, en la que se

establece tener en cuenta los principios de “privacidad desde el diseño” y “privacidad por defecto”, en línea con los receptados en el RGPD (artículo 25).

Entre otras cosas establece (i) contemplar la privacidad en todos los procesos de la organización; (ii) desarrollar aplicaciones con el concepto de la privacidad “por diseño”; (iii) configurar por defecto como “activadas” las opciones de privacidad; (iv) establecer una Política de Privacidad clara y accesible para los titulares, permitir a los titulares el derecho a elegir y controlar los usos que se le da a la información que son de su propiedad, como así también (v) asumir la responsabilidad y designar a un “responsable de privacidad” para el resguardo de los datos personales objeto de tratamiento.

Si bien en la actualidad ni la citada Disposición, ni la Guía resultan obligatorias, en atención a las obligaciones de privacidad a cargo de los responsables en el marco de la Ley 25.326 y la Resolución 4, se entiende que las empresas aplican o deberían estar aplicando procedimientos preventivos de estas características en el marco de su responsabilidad proactiva, como un proceso que genera valor, evitando potenciales costos reputacionales y fidelizando a los clientes o consumidores.

Por otra parte, se observa que pese a que la Guía de Evaluación de impacto se concibe como un documento con recomendaciones y buenas prácticas en materia de privacidad por diseño, la que podría ser solicitada ante un reclamo planteado por los interesados ante la autoridad o bien, en el marco de una investigación de oficio, de acuerdo a la Resolución 4 y el derecho de acceso ya analizado.

En conexión con lo anterior, es dable destacar, la AAIP tiene entre sus competencias y facultades la de solicitar “[f]iscalizar la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos”.

Por su parte, el Proyecto de Ley (2018) establece en su artículo 40 la obligatoriedad de una evaluación de impacto relativa a la protección de los datos en los siguientes casos, sin perjuicio de otros que pueda establecer:

(i) Evaluación sistemática y exhaustiva de aspectos personales de personas humanas que se base en un tratamiento de datos automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas humanas o que les afecten significativamente de modo similar; y (ii) cuando se realice tratamiento de datos sensibles a gran escala, o de datos relativos a antecedentes penales o contravencionales".

Por otra parte, su artículo 42 en la misma línea que el RPDP, establece que "[e]l responsable del tratamiento debe informar a la autoridad de control antes de proceder al tratamiento de datos cuando una evaluación de impacto relativa a la protección de los datos muestre que el tratamiento de datos entrañaría un alto riesgo, pudiendo la autoridad iniciar una investigación de oficio".

Se advierte en este punto que la Ley 25.326, posee una falencia que sería deseable mejorar, puesto que la obligación de realización de evaluaciones de impacto está asociada a derechos fundamentales que podrían presentar un alto riesgo. Es decir, en la actualidad, las empresas no tienen formalmente la obligación de realizar las evaluaciones de impacto o solicitar autorizaciones a la AAIP. No obstante, aunque la tuviesen, ésta podría ser fácilmente "ocultable", tal como han advertido los autores en los apartados anteriores al analizar las dificultades de aplicación práctica del RGPD.

En base a lo analizado, se entiende que el criterio de la normativa actual apunta hacia la responsabilidad proactiva, o en su caso, a la investigación de oficio de la autoridad de control en los casos puntuales que se consideren pueden implicar un alto riesgo a derechos fundamentales.

Al momento, no se han registrado casos de reportes de organizaciones ante la AAIP sobre cuestiones vinculadas a altos riesgos y evaluaciones de impacto.

4.8. Transferencias internacionales y aplicación extraterritorial

Es importante hacer notar que, en el caso de transferencias internacionales, la obligación de rendición de cuentas asegurando garantías adecuadas de privacidad y

seguridad, se encuentra actualmente contemplada en la legislación argentina, mediante: (i) la Disposición DNPDP 60/2016 (aprobó una lista de países que brindan un nivel adecuado de protección de datos personales, la cual es revisada periódicamente, actualizada mediante Resolución AAIP No. 34/2019; y (ii) Resolución AAIP 159/18 (aprobó un conjunto de lineamientos sobre Normas Corporativas Vinculantes a ser utilizadas por empresas como base legal que permite transferencias internacionales de datos personales dentro de un grupo económico).

Una novedad del Proyecto de Ley (2018) es que explícitamente determina que la carga de la prueba en el cumplimiento en materia de transferencias internacionales recae, en todos los casos, en el responsable del tratamiento que transfiere (art. 25), siendo receptado expresamente el principio de responsabilidad proactiva (artículo 10), en línea con el del RGPD.

En este punto, en función de la aplicación extraterritorial del RGPD, algunas empresas argentinas podrían ser susceptibles de tener que aplicar algunas de sus prescripciones, lo que deberá ser analizado de manera pormenorizada en cada caso en particular para determinarse.

En efecto, las Directrices relativas al ámbito territorial del Reglamento 2016/679. (Europea, U., 2018) toman en consideración el “Criterio de Direccionamiento o Targeting” para determinar su aplicación extraterritorial en cuanto al ofrecimiento de bienes o servicios a titulares de datos y/o el monitoreo del comportamiento de los titulares de datos que puede incluir actividades como publicidad orientada a partir del comportamiento del titular, seguimiento en línea (cookies) y encuestas de mercado, que se enfoca no solo en el tratamiento de los datos personales, sino también en la actividad a la cual dicho tratamiento se encuentra vinculada.

En el marco de la Disposición DNPDP 60/16 relativa a transferencias internacionales, se dispone explícitamente la responsabilidad de los exportadores de datos de las disposiciones de la Ley N° 25.326 relacionadas con el tratamiento de sus datos personales, en particular lo relativo a los derechos de acceso, rectificación, supresión y demás derechos, como así también someterse a la jurisdicción argentina, tanto en sede judicial como administrativa.

En la práctica, Peruzotti, M. (2021) resalta que la "[t]endencia que se afianza en la región es la extensión del alcance territorial de las normas en materia de protección de datos. Siendo que las cuestiones relativas a la privacidad de datos se encuentran íntimamente relacionadas con las tecnologías de la información y las comunicaciones, no resulta extraño que se adopten soluciones que propendan a traspasar las fronteras nacionales y aplicar la ley local en forma extraterritorial".

Existen antecedentes jurisprudenciales nacionales que han fallado en línea con el reconocido antecedente del Tribunal de Justicia Europeo "Google Spain SL y Google Inc. vs. Agencia Española de Protección de Datos (AEPD) y Mario Costeja Gonzáles" (2014). En resumidas cuentas, en este caso se consideró que, la vinculación entre entidades de un mismo grupo económico -que intervienen de distinta forma en un negocio común-, deriva en la aplicación de la ley local. Por ejemplo, Google Inc. gestiona técnica y administrativamente Google Search, y la promoción de espacios publicitarios que se da en Google Spain de la que es responsable para España, deviene en la aplicación de la normativa local.

A nivel nacional, se han dado antecedentes sentando el mismo criterio, los que han sido aplicados tanto por los tribunales judiciales y por la autoridad de datos a nivel nacional, la Agencia de Acceso a la Información Pública (fallos "P. A. E. c. Facebook Argentina SRL s/ medida autosatisfactiva" de la Cámara Federal de la Provincia de Mendoza de mayo de 2019 y Resolución de la Agencia de Acceso a la Información Pública "Giolito c. Google Argentina SRL y Google LLC" respectivamente).

A su vez, los estándares de la Red Iberoamericana de Protección de Datos Personales (2017) de los que la AAIP es Estado miembro, prevén una disposición específica que proponen la extensión territorial de las normas de protección de datos a los procesamientos realizados inclusive por responsables o encargados de tratamiento ubicados fuera de las fronteras del propio país (Principio 5.1, inciso d).

4.9. Instrumentos internacionales

El 25 de febrero de 2019, la Argentina ratificó el Convenio para la Protección de las Personas con respecto al tratamiento automatizado de datos de carácter personal y su protocolo adicional, suscripto en la ciudad de Estrasburgo, Francia, el día 28 de enero de 1981 del Consejo de Europa (Convenio 108), aprobado a nivel nacional por la Ley 27.483.

Este Convenio, en su artículo 6 determina que "[l]os datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a condenas penales".

Además, nuestro país ha suscripto el Convenio 108 para la Protección de las Personas con respecto al Tratamiento Automático de Datos Personales o "Convenio 108 modernizado", el que garantiza gran parte de los derechos del RGPD analizados. Si bien este Convenio a nivel nacional ha sido aprobado por la Cámara de Senadores, aún su ratificación se encuentra pendiente de formalización.

En forma complementaria, cabe referir que las Directrices de la OCDE (2011) sobre prácticas empresariales responsables plantean:

- la elaboración de evaluaciones de impacto,
- información transparente,
- responsabilidad extraterritorial,
- "[e]jercer la debida diligencia en materia de derechos humanos en función de su tamaño, naturaleza y contexto de sus actividades y de la gravedad de los riesgos de impactos negativos"
- "[c]ooperar para poner remedio a los impactos negativos sobre los derechos humanos, cuando se descubra que han causado dichos impactos o que han contribuido a generarlos"

- facilitar el acceso a los consumidores a “[m]ecanismos extrajudiciales, de resolución de conflictos y a medidas correctoras equitativas, fáciles de utilizar, rápidas y eficaces, sin costos ni cargas innecesarias”.

Si bien Martínez (2020) destaca que estas Directrices no son vinculantes, los Estados adherentes se comprometen a promover su uso y a establecer Puntos Nacionales de Contacto. Cabe mencionar que entre los países adherentes se encuentra Argentina.

Asimismo, cuarenta y dos países -entre los que se encuentra Argentina- han suscrito en el 2019 los Principios de la OCDE sobre la Inteligencia Artificial para la transición digital para el desarrollo sostenible, entre los que se estableció que los sistemas de IA de los Estados deberán:

- estar presididos por la transparencia y divulgación responsable, a fin de garantizar que las personas sepan cuándo están interactuando con ellos y puedan oponerse a los resultados de esa interacción;
- permitir la intervención humana cuando sea necesario, para garantizar una sociedad justa y equitativa;
- funcionar de manera fiable y los potenciales riesgos deberán evaluarse y gestionarse en todo momento; y
- Las organizaciones y las personas que desarrollen, desplieguen o gestionen sistemas de IA deberán responder por su correcto funcionamiento en consonancia con los principios precedentes.

De lo expuesto se advierte que, las prácticas empresariales de Responsabilidad Social Corporativa y de IA adheridas por varios Estados en el marco de la OCDE, guardan varios en puntos en común con los principales principios y salvaguardas jurídicas analizadas en el marco del RGPD y normativa nacional para la protección de los datos personales.

4.10. Reparación del daño

En el ámbito local, los efectos jurídicos perniciosos podrían configurar daños morales y materiales. Por ejemplo, entre los morales, se conciben riesgos a derechos fundamentales que gozan de protección en la Constitución Nacional (igualdad, no discriminación, libertad religiosa, libertad personal, intimidad, libertad de expresión, condiciones de igualdad, tutela judicial efectiva, legalidad penal, educación, libertad de sindicación, derecho de petición, entre otros).

La carga de la prueba tanto en el plano judicial - sede civil o penal-, como en el plano administrativo -AAIP-, estará en cabeza del responsable de tratamiento (organización en particular), en coherencia con el principio de responsabilidad proactiva, información y transparencia. Esto resulta positivo para posibilitar la presentación de reclamos por parte de los afectados, ya que poner la carga de la prueba sobre los usuarios sobre este tipo de operaciones internas de las organizaciones, dificultaría todo tipo de reclamo, y por ende, reparación.

A nivel judicial, podría ser de aplicación el art. 377 del Código Procesal Civil y Comercial de la Nación que establece que "[i]ncumbirá la carga de la prueba a la parte que afirme la existencia de un hecho controvertido o de un precepto jurídico que el juez o el tribunal no tenga el deber de conocer. Cada una de las partes deberá probar el presupuesto de hecho de la norma o normas que invocare como fundamento de su pretensión, defensa o excepción. Si la ley extranjera invocada por alguna de las partes no hubiere sido probada, el juez podrá investigar su existencia, y aplicarla a la relación jurídica materia del litigio".

Mientras que respecto a la carga de la prueba en el ámbito de la Dirección Nacional de Protección de Datos Personales, el Decreto reglamentario de la Ley 25.326 dispone que "[e]n la misma acta se dispondrá agregar la documentación acompañada y citar al presunto infractor para que, dentro del plazo de CINCO (5) días hábiles, presente por escrito su descargo y ofrezca las pruebas que hacen a su derecho. […] La constancia del acta labrada conforme a lo previsto en este artículo, así como las comprobaciones técnicas que se dispusieren, constituirán prueba

suficiente de los hechos así comprobados, salvo en los casos en que resultaren desvirtuados por otras pruebas".

Granero, H. R. (2019), sostiene que el derecho interno provee mecanismos a las personas para responsabilizar por las afectaciones que se produzcan por daños por tratamientos automatizados. En particular, este autor plantea que la propia esencia del Derecho Civil es la de distribuir las cargas y costos sociales en forma equitativa, por lo que, las "[t]ecnologías que con su accionar pueden exponer a los usuarios a nuevos riesgos e incluso a la efectiva producción de daños, se propicia que éstos deben ser asumidos por quien los brinda, generando una responsabilidad objetiva", por parte de quien lleva una actividad riesgosa, "[c]omo puede ser un algoritmo que efectúe discriminaciones".

Por lo que, expresa que la utilización de tecnologías de IA podrían encuadrarse en el concepto de actividad riesgosa previsto en el artículo 1757 del Código Civil y Comercial de la Nación, por la que debería responder, quien ejecuta la actividad, se sirve u obtiene provecho de ella (artículo 1758).

Por otra parte, el Código Civil y Comercial de la Nación prevé una responsabilidad civil para la prevención del daño de manera obligatoria. Así como resalta Palazzi (2021), se introducen deberes genéricos de conducta que mandan a (i) no dañar (art.1716, CCyC) y a (ii) evitar la causación del daño (art. 1710, CCyC) como una fuente de obligaciones, (iii) legitimando para reclamar a quienes acrediten un interés razonable en la mentada prevención (art. 1712).

En particular, el artículo 1710 dispone que "[t]oda persona tiene el deber, en cuanto de ella dependa, de: a) evitar causar un daño no justificado; b) adoptar, de buena fe y conforme a las circunstancias, las medidas razonables para evitar que se produzca un daño, o disminuir su magnitud; si tales medidas evitan o disminuyen la magnitud de un daño del cual un tercero sería responsable, tiene derecho a que éste le reembolse el valor de los gastos en que incurrió, conforme a las reglas del enriquecimiento sin causa; c) no agravar el daño, si ya se produjo.

Por su parte, el artículo 1711 establece que “[t]odas las personas tanto físicas como jurídicas tienen el deber de evitar cualquier daño previsible a terceros, así como la obligación de adoptar todas las medidas razonables para evitar que se produzca el daño o disminuir su magnitud”.

Ante el incumplimiento, surgirá sobre la cabeza de su autor la correspondiente obligación de reparar (art. 1716, CCyC) o prevenir en concreto (art. 1711, CCyC), según el caso.

La conexión directa con la posibilidad de reparación del daño, será que el derecho de acceso sobre la “lógica sobre la explicación brindada” sea brindado al titular del dato en forma amplia.

CAPÍTULO 5. CUESTIONES PRÁCTICAS

5.1. Casos de derecho comparado de efectos jurídicos perniciosos en tratamientos automatizados

Corvalán, J. G. (2020) analiza a la inteligencia artificial concebida desde sus dos ejes: su “lado luminoso” y su “lado oscuro”.

Al lado luminoso, lo caracteriza por la posibilidad de la IA para “[o]ptimizar y simplificar actividades, […] efectivizar derechos. Por ejemplo, permite asistir a las personas con discapacidad visual, acelera los procesos judiciales, mejora el acceso a políticas sanitarias, entre muchos otros”. Haciendo hincapié en que “[s]i se construyen las condiciones adecuadas, se trata de una oportunidad inédita para mejorar organizaciones y contribuir al cumplimiento de los objetivos de desarrollo sostenible”.

Al “lado oscuro de la IA”, lo asocia principalmente a los riesgos y daños que estos sistemas pueden generar, de los que los seres humanos pierdan su control. Algunos ejemplos que menciona son “[s]esgos, discriminación , vigilancia masiva contraria a los derechos humanos, tratamiento de perfiles digitales contrarios a las leyes, vulneración de los derechos de los trabajadores, entre otras cuestiones”.

Por otra parte, el Libro Blanco sobre la inteligencia artificial (Europea U., 2020) advierte que el uso de IA “[p]uede afectar los valores en los que se basa la UE y dar lugar a violaciones de los derechos fundamentales, incluidos los derechos a la libertad de expresión, libertad de reunión, dignidad humana, no discriminación por motivos de sexo, origen racial o étnico, religión, creencia, discapacidad, edad u orientación sexual […] protección de datos personales y vida privada, o el derecho a un recurso judicial efectivo y un juicio justo, así como protección al consumidor”. Este libro también hace hincapié en que este tipo de sistemas al analizar grandes cantidades de datos e identificar vínculos entre ellos, también “[p]uede usarse para rastrear y anonimizar datos sobre personas, creando nuevos riesgos de protección de datos personales, incluso con respecto a conjuntos de datos que per se no incluyen datos personales”.

Por su parte, la Guía de Gestión de Riesgo y Evaluación de impacto en tratamientos de datos personales de la Agencia Española de Protección de Datos (2021), indica que estos procesamientos automatizados pueden generar daños morales y daños materiales. Los primeros, pueden consistir por ejemplo, en daños psicológicos permanentes, invasión de la privacidad, violación de los derechos fundamentales (discriminación, libertad de expresión), extorsiones, y cyberbullying; mientras que los materiales pueden versar en la adjudicación errónea del dinero del titular de datos a otra persona sin compensación, dificultades financieras a medio o largo plazo, pérdida del trabajo, daño a la propiedad, y/o la pérdida financiera como resultado de un fraude, entre otros.

En este punto, (Ali, M., et. al, 2019) resalta que el enorme éxito financiero de las plataformas de publicidad digital, se debe en parte a las características precisas de orientación de los anuncios que ofrecen, proceso que en muchos casos "sesga" la publicación de formas que los anunciantes no pretenden. Refieren que de sus investigaciones en relación a la empresa Facebook, han concluido que -incluso cuando los anunciantes establecen sus parámetros de orientación para que sean inclusivos-, el presupuesto del anunciante y el contenido del anuncio, contribuyen significativamente al sesgo de la publicación de Facebook, observando un sesgo significativo en la entrega, por aspectos de género y raza, que pueden conducir a anuncios digitales potencialmente discriminatorios.

El Libro Blanco sobre la inteligencia artificial también alerta que los intermediarios de Internet también utilizan la IA para ordenar la información para establecer prioridades y moderar los contenidos, como los buscadores o redes sociales, que pueden afectar los derechos de libertad de expresión, protección de los datos personales y libertad. En este punto, se advierten los siguientes riesgos adicionales (Europea U., 2020).

Por su parte, Martinez (2021) advierte que “[l]os proveedores de servicios como por ejemplo Twitter, Facebook, Whatsapp y Google controlan los contenidos de sus usuarios, o sea, controlan la conducta de cientos de millones de personas. Eso

implica en definitiva, analizar y saber lo que esas personas dicen y piensan". Resaltando que en algunos casos, estas empresas también [r]estringen la capacidad de difusión o interacción de determinados usuarios o directamente los bloquean […]".

El pasado 21 de junio, el Supervisor Europeo de Protección de Datos y el Comité Europeo de Protección de Datos han pedido "[u]na prohibición general de cualquier uso de la IA para el reconocimiento automático de rasgos humanos en espacios de acceso público, como el reconocimiento de rostros, marcha, huellas dactilares, ADN, voz, pulsaciones de teclas y otras señales biométricas o de comportamiento, en cualquier contexto". Y al mismo tiempo, han referido que "[c]onsideran que el uso de IA para inferir las emociones de una persona física es muy indeseable y debería prohibirse" (Comité Europeo de Protección de Datos, 2021).

1. Discriminaciones de precios - Amazon

Los autores Serrano, E., Such, J. M., Botía, J. A., & García-Fornes, A. (2014) refieren que la elaboración de perfiles de compradores es frecuentemente utilizada en el comercio electrónico y puede ser utilizada para realizar discriminaciones de precios. Explican que esta técnica puede consistir en "[c]obrar a los clientes precios diferentes por el mismo bien de acuerdo con los perfiles de los clientes, es decir, si un vendedor sabe que un bien es de gran interés para un cliente, el vendedor podría cobrarle a este cliente más dinero por este bien que a otros clientes por el mismo bien."

Citan como ejemplo que en el año 2000, la empresa Amazon cobró a los clientes precios diferentes por los mismos títulos de DVD. Cuando la historia trascendió, la empresa afirmó que era parte de una prueba de precios y suspendió esta práctica.

Ezrachi, A., & Stucke, M. E. (2016) proponen una posible teoría del daño en torno a la discriminación de precios basada en el uso de precios algorítmicos. Exploran cómo la personalización de nuestro entorno online a través de las búsquedas, las compras previas o el envío de correo electrónico, afecta a la dinámica de la competencia y al bienestar del consumidor. Los autores observan que la

discriminación basada en el comportamiento también puede reducir su bienestar, ya que la "individualización" no se detiene en las promociones, sino que afecta además a las decisiones de precios, de modo que los más vulnerables, en muchas ocasiones terminan pagando más.

En este punto, cabe destacar que en el Libro blanco sobre la inteligencia artificial del Consejo Europeo, refiere que "[l]os agentes económicos siguen siendo plenamente responsables de que la IA respete las normas existentes en materia de protección de los consumidores. Igualmente, debe prohibirse todo uso de los algoritmos con relación al comportamiento de los consumidores cuando se vulneren las normas existentes, y tales vulneraciones deben sancionarse en consecuencia".

A continuación, se detallarán sin ánimo exhaustivo algunos casos de derecho comparado a modo de ilustrar algunos efectos jurídicos negativos que pueden tener lugar en el marco de los procesamientos automatizados objeto de estudio.

2. Publicidad sesgada en función de raza, género y religión - Facebook

En 2019, el Departamento de Vivienda y Urbanismo de EE. UU. demandó a la red social Facebook tras descubrir que su algoritmo de publicidad poseía un sesgo algorítmico de recomendación que ofrecía acceso desigual a anuncios en función de la información demográfica de sus usuarios (Karen H., 2019).

Por ejemplo, se mostraban principalmente a mujeres anuncios de búsqueda de profesionales de educación infantil y de secretarias, mientras que las publicaciones para empleo de conserje y taxista, se mostraban en mayor proporción a personas de grupos minoritarios. Además, anuncios sobre venta de viviendas eran mostrados a usuarios blancos, mientras que, anuncios de alquileres eran más mostrados a las minorías en comparación que los anuncios sobre ventas de propiedades.

3. Discriminación laboral por género - Amazon

En 2014 Amazon diseñó una herramienta de contratación que revisaba currículums de los solicitantes de empleo con el objetivo de mecanizar la búsqueda de los

mejores talentos. En 2015, la compañía se dio cuenta que este sistema no calificaba a los candidatos de una manera neutral al género. Esto se debió a que los modelos informáticos de Amazon fueron capacitados para examinar a los solicitantes mediante la observación de patrones en los currículums enviados a la empresa durante un período de 10 años y la mayoría provenía de postulantes hombres (Huang, Z., 2021)

4. Prioridad de contenidos automatizados - “Palabras clave” motor de búsqueda Google

La profesora de Harvard Latanya Sweeney ha presentado un estudio en el que identifica prejuicios raciales en los resultados de búsquedas de Google. Advierte que, al introducir un nombre utilizado mayoritariamente por personas de raza negra, se observa un mayor número de anuncios relacionados con actividades delictivas.

Sin embargo, se ha destacado que Google no es totalmente responsable de los resultados, dado que en gran medida éstos se deben a un posible reflejo de conductas de búsqueda como causa de discriminación de usuarios, como de anunciantes (ABC, 2013).

5. Discriminación racial - Etiquetado de fotos - Google Chrome OS

En 2015, Google tuvo que disculparse porque su propio software de inteligencia artificial de etiquetado automático de fotos, etiquetó erróneamente la foto de dos personas afroamericanas como “gorilas” (BBC Mundo Tecnología, 2015).

6. Publicidad política - Facebook

En 2018, Facebook pagó 5 mil millones a la Comisión Federal de Comercio de EE. UU, la multa más grande registrada por violar las leyes de privacidad, dado que se reveló que la empresa británica Cambridge Analytica utilizó su aplicación en la red social para acceder a los datos personales de 87 millones de usuarios en todo el mundo y configurar publicidad política, especialmente durante la campaña

presidencial estadounidense de 2016 y el referéndum de adhesión a la Unión Europea del Reino Unido (BBC News, 2019).

7. Recopilación automatizada de datos de ubicación - Google Chrome OS

De acuerdo con una sentencia de un tribunal australiano en 2021, se determinó que la recopilación automatizada de datos de ubicación realizada por Google en teléfonos Android, ha sido "parcialmente" engañosa, puesto que si un cliente marcaba que no deseaba que se realice la recopilación de su "Historial de ubicaciones", pero dejaba activada la "Actividad web y de aplicaciones", la empresa continuaba recopilando estos datos (Zhou, N., 2021).

8. Moderación de contenidos automatizados en Youtube - “Discursos del odio”

Right Wing Watch, publicó videos en la plataforma de Youtube, que contenía ejemplos de supuestos discursos de odio y discriminación (David I., 2021).

En forma posterior, recibió un aviso de una prohibición permanente relacionada con violaciones de las reglas de Youtube.

Más tarde, Youtube reconoció el error, reinstaló el servicio y atribuyó el error al “gran volumen de videos en su sitio”. La prohibición realizada evidencia una preocupante incapacidad de YouTube para distinguir entre los creadores de contenido prohibido, de los que intentan contrarrestarlo.

En un comunicado, Right Wing Watch expresó: "[n]uestros esfuerzos para exponer la opinión intolerante y las teorías de conspiración peligrosas difundidas por activistas de derecha, ahora dan como resultado que YouTube prohíba nuestro canal y elimine miles de nuestros videos".

9. Asistente de Google

La compañía estadounidense ha comparecido el 29 de junio de 2021 ante el Comité de Información y Tecnología del Parlamento de India, donde habría admitido que en

ocasiones sus empleados escuchan las grabaciones que lleva a cabo el Asistente de Google (India today, 2021).

A la pregunta del diputado de BJP, Nishikant Dubey, del Comité Parlamentario Permanente de Tecnología de la Información sobre si sus empleados escuchan algunas grabaciones de los usuarios con el Asistente de Google, el equipo de la empresa admitió que a veces el Asistente de Google graba audios en un teléfono inteligente, incluso cuando un usuario no ha activado la herramienta de Inteligencia Artificial con un comando de voz como 'Ok, Google'.

Los representantes de Google han asegurado que la grabación de audio no afecta a la información sensible de los usuarios, y que solo se escuchan conversaciones generales, aunque no han explicado cómo diferencian entre qué información es sensible y cuál no.

No obstante, el panel del Parlamento, encabezado por el diputado de Lok Sabha, Shashi Tharoor, cree que la grabación de las conversaciones del Asistente de Google es una violación de la privacidad y el informe final del Panel hará recomendaciones al gobierno al respecto.

10. Identificación de Datos biométricos - Clearview IA

La empresa Clearview IA, con sede en Estados Unidos ha sido sancionada por la Autoridad de Protección de Datos de Hamburgo (DPA) a raíz de la denuncia presentada por un ciudadano que solicitó la eliminación de sus imágenes y de los valores hash matemáticos que representan su perfil biométrico en las bases de datos de la compañía (One Trust Hamburgo, 2021).

La empresa ha extraído fotos de sitios web o redes sociales públicas y ha creado una base de datos de perfiles biométricos sin conocimiento de los usuarios, a la que luego se le aplicaba reconocimiento facial. La base de datos tendría más de 3.000 millones de imágenes. Según se ha informado, el acceso a la base de datos se vendió a empresas privadas y fuerzas de vigilancia estadounidenses.

La DPA ha ordenado a Clearview AI que elimine los valores hash matemáticos que representan el perfil biométrico del denunciante y que confirme la eliminación, la que debería ser implementada antes del 12 de febrero de 2021.

5.2. Efectos del RGPD y responsabilidad proactiva

Tal como hemos señalado, Argentina ha seguido los estándares europeos en su proyecto de Ley (del 2017 y del 2018) y ha sido considerado país adecuado por el Consejo Europeo. Por las razones anteriores, resulta de utilidad observar el estado de situación de la aplicación práctica del RGPD, en relación a la responsabilidad proactiva en la gestión de la información en organizaciones.

El Reglamento Europeo fue adoptado en abril de 2016 y ha entrado en vigor desde el 25 de mayo de 2018. Desde su sanción se han producido innumerables efectos positivos a nivel global, principalmente concebido como el principal estándar global de privacidad.

A continuación, se mencionarán brevemente algunos comentarios sobre los efectos de su implementación reportados por distintos expertos de países desarrollados.

En principio, es dable mencionar que al margen de las fortalezas del RGPD, se han planteado varias dudas sobre su aplicación efectiva, puesto que en muchos casos la normativa planteó grises y mecanismos abiertos que en algunos casos dificultan su armonización, los que han sido clarificados con diversas directrices (The Technolawgist, 2019).

Otra debilidad planteada, es que algunas previsiones del RGPD han tenido el efecto contrario al perseguido. Por ejemplo, las exigencias sobre mayor transparencia al deber de información han derivado en muchos casos en políticas de privacidad aún más extensas y menos claras para los usuarios (Sara Fernandez, The Technolawgist, 2019).

Algo similar se manifiesta que ha sucedido respecto al pedido masivo de autorización de cookies, lo que dejó en evidencia la urgente necesidad a nivel global de adoptar nuevas configuraciones de privacidad y consentimiento más efectivas en la recolección de datos (Marie Potel Saville, The technolawgist, 2019).

Se advierte que, si bien el RGPD está cada vez más vigente en los países desarrollados y las empresas han realizado un gran esfuerzo para implementarlo, "[a]ún queda mucho por hacer: las empresas deberían pasar de un enfoque sobre la privacidad puramente de compliance, estilo "tick in the box", al desarrollo de la experiencia de usuario entorno a la privacidad, incluso convirtiéndola en una ventaja competitiva. Para ello es necesario invertir en herramientas que puedan ayudar a los consumidores a gestionar sus datos de forma sencilla" (Sara Fernandez, The Technolawgist, 2019).

También se han planteado dificultades en la gestión de la privacidad por diseño realzando que "[l]a estandarización técnica para concretos tratamientos (e.g. para hardware empleado en tratamientos de IoT), así como regulación específica para determinados sectores (e.g. investigación con datos de salud, marketing online, etc.), serán medidas de utilidad para una correcta aplicación del GDPR y de la LOPD". "[A]ún hay mucho camino por recorrer en la era del big data y el machine learning". (Ivana Bartoletti, The technolawgist, 2019).

Respecto a las sanciones del RGPD, Barrett (2020) ha reportado cambios en la ubicación de varias empresas con la finalidad de reducir la probabilidad y/o severidad de las multas; mientras que otros especialistas resaltan que "[a]unque las sanciones sean elevadas, sucede que en muchos casos la ganancia obtenida por el manejo de datos personales en violación de RGPD es mayor que la multa que pudiera imponerse" (Ana Paula Rumualdo, The technolawgist, 2019).

De lo expuesto, se observa que si bien los países desarrollados han implementado la normativa actualizada en materia de protección de datos personales hace 3 años -la que posee garantías suficientes en virtud del art. 22 ante procesamientos automatizados-, se advierten diversas dificultades en su aplicación práctica y

desafíos pendientes por ejemplo en la gestión de algoritmos, recolección de datos, cookies, deber de información y responsabilidad proactiva.

Elizabeth M. Renieris (The technolawgist, 2019) resalta que “[n]o existe una medida única, ninguna pieza de legislación, acción administrativa, tecnología o solución de mercado, que pueda proporcionarnos una mejor relación con nuestros datos a nivel de individuos, de empresas, de gobiernos y de sociedad global. El progreso será exponencial y requerirá una base de leyes, ajustes de mercado y cambios de comportamiento. Lo más importante es no aceptar una versión derrotista del futuro donde no tengamos control sobre cómo se usan los datos para impactar en nuestras elecciones o decisiones”.

De todo lo expuesto, se observa que si bien la normativa resulta un eslabón fundamental para garantizar un cumplimiento efectivo, la gestión de la privacidad por diseño requerirá un cambio de paradigma y de comportamiento, asociado al valor compartido como ventaja competitiva a largo plazo.

5.3. El rol del deber de información para el ejercicio y tutela de derechos

De la observación de diversas Políticas de Privacidad de empresas que prestan servicios en Argentina en la actualidad, se concluye que existe una tendencia generalizada al incumplimiento del deber de información.

Lo más preocupante es que en Argentina, este deber de información resulta obligatorio desde hace más de 20 años, de conformidad con el artículo 6 de la Ley 25.326, el que ha sido analizado en los apartados anteriores. Y que este consentimiento es la base legal por excelencia para el tratamiento de los datos de los usuarios, o parte de la relación contractual que une al titular del dato con determinada organización.

Tal como advierte Esteban Ruiz Martinez (2021) "[s]i bien el derecho a la protección de los datos personales está cada vez más vigente en las normativas de los países más desarrollados, está ausente en su aplicación concreta […]". En particular, señala que “[e]sta deficiencia afecta tanto el derecho a la intimidad como el derecho

a la autodeterminación informativa, estratégicos para nuestro desarrollo como personas en el mundo actual, legitimantes de los sistemas de gobierno".

Como se ha analizado en los apartados anteriores, tanto en el marco del RGPD como de la legislación nacional, el cumplimiento efectivo de este deber es fundamental principalmente porque varias empresas justifican su base legal de procesamiento en este contrato de adhesión ("consentimiento explícito del usuario" y/o "relación contractual"), cuando la información comunicada en general es deficiente o excesiva en cuanto a las finalidades informadas.

Se advierte además, que a menudo no se incluye información clara y transparente; o que no se les informa correctamente a los usuarios cuestiones básicas tales como, la Ley de privacidad aplicable en su jurisdicción, o los datos de contacto de la autoridad nacional en el caso que el titular necesitara pedir asistencia o presentar un reclamo para proteger sus derechos afectados.

La falta de información adecuada se traduce en que varios usuarios argentinos no están al tanto de los derechos que poseen realmente (muchas veces no se detallan), ni de la posibilidad de solicitar asistencia a la autoridad local (muchas veces no se detalla). En muchos casos, tampoco se suministra a los usuarios "formas de contacto" para el ejercicio de los derechos garantizados actualmente en la legislación Argentina, mediante la Ley 25.326.

En este contexto, resulta difícil imaginar una rendición de cuentas por parte de organizaciones multinacionales informando y explicando a los usuarios qué procesamientos específicos de datos automatizados realizan, suministrando un medio ágil para oponerse a los mismos, o explicando la lógica empleada en sus algoritmos, si que previamente no han asumido valores de responsabilidad proactiva en los principios más básicos de este deber en sus Políticas de Privacidad.

El cumplimiento del deber de información del art. 6 de la Ley 25.326, tiene un rol esencial por su estrecha relación con la posibilidad de ejercicio de los derechos ante procesamientos automatizados, a través del derecho de acceso para una

explicación sobre la lógica empleada, por ejemplo, tal como ha sido analizado en detalle en los capítulos anteriores.

La segunda falencia es que a menudo, las Políticas de Privacidad suelen determinar la jurisdicción y normativa aplicable en el extranjero. Esto lleva a que, en muchos casos, las grandes empresas obstaculicen o limiten su responsabilidad ante titulares de datos radicados en Argentina.

En este contexto, hay empresas que no habilitan en general -aún en este contexto hiperconectado- formas accesibles, prácticas y no onerosas, de recepción de consultas o reclamos por parte de los ciudadanos en las jurisdicciones donde operan. Por el contrario, en general se suministran formularios o respuestas automatizadas limitadas de información, lo que deja dos alternativas a los afectados: asumir altos costos para emplazarlas, o desistir de la acción.

Es evidente que estas trabas desincentivan de por sí la presentación de denuncias ante autoridades locales, debilitando así, el incipiente empoderamiento de los ciudadanos ante la protección de sus datos, lo que en espiral termina repercutiendo en la falta de incentivos de las empresas para ser más proactivos en las salvaguardas implementadas.

La tercera falencia observada es que muchas empresas realizan perfilados y predicciones en sus operaciones de marketing digital, sin embargo luego no informan claramente que llevan adelante estos tratamientos en sus Políticas de Privacidad. Esto lleva a la consiguiente dificultad de los titulares de datos de estar informados sobre qué empresa pudo realizar un procesamiento automatizado o perfilado sobre su persona, para después poder ejercitar los derechos que se han analizado a lo largo del presente trabajo.

Por último, resulta dificil confiar en que las empresas actuarán con responsabilidad proactiva internamente en sus organizaciones, por ejemplo, realizando evaluaciones de impacto (al momento, una buena práctica) o informando a sus usuarios cuál fue la lógica de una decisión empleada, si previamente no se ha dado cabal cumplimiento al deber de información (art. 6 de la Ley 25.326).

Se observa la urgente necesidad de sanción del Proyecto de Ley (2018) para generar mayores incentivos en las organizaciones respecto a su responsabilidad proactiva en la gestión de la información y sería saludable que éstas puedan presentar consultas a la Autoridad de control en el caso de generarse un riesgo residual elevado en sus procesamientos, de modo de encarar un trabajo colaborativo preventivo.

6. CONCLUSIONES

Recordemos las preguntas que nos planteáramos al comienzo del trabajo: ¿Existen elementos jurídicos en la normativa vigente que habiliten a los titulares de datos a solicitar explicaciones ante las empresas -cuando una decisión automatizada o perfilado- le produzca efectos jurídicos negativos?

Los fundamentos de la bibliografía analizada y las entrevistas que se han realizado en el presente trabajo, permitieron efectuar un análisis del estado actual sobre las posibilidades de actuación que tendrían los titulares de datos y la autoridad de control nacional, frente a afectaciones de derechos humanos en el marco de procesamientos automatizados y perfilados en Argentina.

Son muchos los desafíos pendientes en América Latina para generar el entorno propicio que pueda maximizar las oportunidades por sobre los riesgos.

En principio, es importante subrayar que, por supuesto que resulta más que urgente la necesidad de actualización de la Ley Argentina con disposiciones claras sobre estas complejas cuestiones, siendo además necesaria la ratificación del Convenio 108 modernizado, circunstancias que influirán en el status de nuestro país ante una eventual revisión de adecuación por parte del Consejo Europeo.

Sin perjuicio de ello, hasta que alguna de estas normativas finalmente sean sancionadas, será fundamental que la autoridad nacional pueda continuar cumpliendo con sus competencias y deberes del artículo 19 de la Ley 27.275, con el "[o]bjeto de velar por el cumplimiento de los principios y procedimientos establecidos en la presente ley [...]", como así también, "[f]iscalizar la protección integral de los datos personales [...] para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre".

En particular, del presente estudio se desprende que, de manera independiente a la necesidad de actualización de la Ley 25.326, y de la discusión sobre si las últimas resoluciones dictadas por la Agencia de Acceso a la Información Pública (AAIP)

tienen el carácter de “obligatorias” o de “buenas prácticas”; de la materia normativa nacional, se derivan los principales pilares para garantizar el ejercicio de derechos ante afectaciones en el marco de perfilados y decisiones automatizadas.

La normativa argentina con sus resoluciones y buenas prácticas, le otorga un rol protagónico y amplio a la responsabilidad proactiva de las organizaciones en la protección de los datos personales, la que en su caso, deberá ser demostrada exhaustivamente ante una investigación de oficio de la autoridad de control, o bien ante el reclamo de los interesados.

Por lo que se concluye que, los usuarios que se vean afectados por estos procedimientos poseen en la actualidad elementos jurídicos para presentar reclamos ante las organizaciones que no cumplan con los plazos dispuestos en la Ley 25.326 asociados al derecho de acceso, rectificación o supresión, en relación a la explicación sobre la lógica empleada, de conformidad con la Resolución AAIP 4 analizada y los estándares internacionales de la materia.

Asimismo, la autoridad de control, es decir la Agencia de Acceso a la Información Pública (AAIP) podrá recepcionar reclamos de titulares, e iniciar las investigaciones de oficio que considere pertinentes, como proceder a la aplicación de sanciones en atención a sus competencias y facultades.

En el mientras tanto, será primordial la búsqueda de mecanismos de mayor colaboración entre empresas multinacionales y la autoridad de control nacional, para comenzar a dialogar y trabajar en este punto mucho más proactivamente que lo que ocurre hoy día, sin que se acuda al argumento que la ley en la actualidad, no lo exige explícitamente.

Si bien del presente trabajo no se han reportado antecedentes específicos a nivel nacional sobre estas cuestiones, es esperable que, en el mediano o corto plazo, los ciudadanos comiencen a presentar reclamos ante las empresas, o bien, soliciten la asistencia de la autoridad de control.

La segunda pregunta que planteamos al inicio de este estudio fue si la actualización de normativa en materia de datos personales será suficiente para lograr la responsabilidad proactiva en organizaciones respecto a la gestión de la información.

Tras haber analizado las dificultades prácticas que plantea el RGPD a nivel global, consideramos que, las garantías legales formales, -como podría ser la sanción de una ley actualizada en Argentina-, si bien fortalecerán el ecosistema de privacidad con cláusulas explícitas sobre alcance extraterritorial y multas pecuniarias más elevadas, por ejemplo; se advierte que por sí sola no alcanzará para proteger los datos personales frente a este tipo de tecnologías tan avanzadas y de complejidad.

Tal como hemos visto en el presente trabajo, la experiencia a nivel mundial ha demostrado que, aún en los países más desarrollados con normativas actualizadas al RGPD, existen múltiples desafíos pendientes para garantizar adecuadamente los derechos de los titulares ante mecanismos automatizados. Aún queda mucho trabajo por hacer en cuanto a estos tratamientos.

Las complejidades planteadas dejan en claro que, la cooperación de las autoridades de datos a nivel global, será un eslabón clave para aclarar los grises de la normativa, como así también, para alinear interpretaciones ante los innumerables retos que la adopción de la IA plantea y seguirá planteando a los Estados, empresas y ciudadanos.

Desde ya que los mecanismos de control de la AAIP y el mayor conocimiento y capacitación de los usuarios sobre sus derechos, resultan fundamentales para lograr mayores incentivos en el cumplimiento de la normativa.

La tercera pregunta que nos planteamos fue cuál es el rol del deber de Información para la tutela efectiva de los derechos consagrados en el marco del art. 22 del RGPD.

Del presente trabajo quedó evidenciado que el principio de responsabilidad proactiva no puede ser concebido sin el deber de información, transparencia, y rendición de cuentas, elementos por excelencia constitutivos del consentimiento.

La responsabilidad proactiva se posiciona de la mano con el deber de información como el nuevo paradigma de la privacidad y como la herramienta más eficiente ante estos tratamientos, ya que aplica de forma transversal en todas las organizaciones y a todas las fases de tratamiento, cualquiera sea su modelo de negocio, incluyendo de este modo cualquier opacidad de la IA que, no resulte fácil de detectar.

Asimismo, la transparencia en la gestión de la información es esencial para la rendición de cuentas ante pedidos de acceso en el marco del art. 14 de la Ley 25.326 para obtener mayores detalles sobre la explicación sobre la lógica empleada en dichos procesamientos, o bien, en el caso de supresión o rectificaciones del art. 16 de la mentada normativa.

Por otra parte, el deber de información en Políticas de Privacidad de las empresas resultan fundamentales para que los usuarios sean conscientes de sus derechos, y para que los titulares estén al tanto que la autoridad de control nacional puede brindarles asistencia en caso de afectaciones y respuestas insuficientes por parte de las organizaciones. El deber de información se posiciona como el eje inicial del ejercicio y tutela de derechos, rendición de cuentas y para una eventual reparación posterior en sede civil, de corresponder.

Por lo que, resulta primordial que las principales empresas globales con alcance masivo que operan en distintos países de Latinoamérica, asuman de una vez su deber de información en sus Políticas de Privacidad de manera diligente, dando cuenta de los procesamientos automatizados que efectúan, así como las alternativas existentes para una tutela efectiva jurídica en cada jurisdicción particular en las que operan.

Sin mecanismos claros de información y ejercicios accesibles para el ejercicio de los derechos, resulta imposible imaginar la proactividad de las organizaciones en la gestión de la información ante tratamientos automatizados, como su colaboración con interesados y autoridades locales en los derechos asociados al art. 22 del RGPD, aplicables en Argentina mediante la Resolución AAIP 4.

6.1. RECOMENDACIONES

Será clave que las organizaciones puedan comprender que, cada vez más las ventajas competitivas y el mejor posicionamiento a largo plazo frente a los competidores, estará dado por una adecuada protección de los datos personales, siendo confianza y transparencia fundamentales como valor compartido. Prueba de esto, es que con mayor frecuencia las organizaciones que no adoptan medidas eficientes de protección, se ven afectadas por falta de reputación y/o incidentes de seguridad con implicancias en sus principales activos: clientes, información, reputación y su valor de mercado.

Para fortalecer la responsabilidad en materia de datos en Argentina consideramos que se necesitará: (i) una autorregulación responsable y proactiva por parte de las empresas con mayor énfasis en las áreas de Marketing y Publicidad; (ii) el fortalecimiento de la autoridad de control, para que pueda hacer seguimiento activo y enforcement de estas complejas cuestiones en conjunto con las organizaciones y brindando apoyo a los ciudadanos; y (iii) fomentar la educación y concienciación de los titulares de datos en la defensa de sus datos personales e intimidad.

Si bien son muchos los frentes que atender y las preguntas que quedan por aclarar, se detectan al menos tres herramientas que podrían colaborar al fortalecimiento de las cuestiones antes descriptas.

En principio, y si bien la AAIP no ha dejado de estar en funcionamiento tras la renuncia de su director anterior, Eduardo Bertoni -la que se hizo efectiva el 1 de enero de 2021-, resulta esencial la designación formal de un nuevo Director de la Agencia de Acceso a la Información Pública, conforme los requisitos que impone el artículo 20 de la Ley 27.275. Tal como se mencionó en el apartado anterior, los nuevos desafíos requieren una autoridad de control fortalecida para poder hacer frente a los múltiples desafíos existentes.

Por un lado, el trabajo de Puntos Nacionales de Contacto para el desarrollo sostenible constituidos por los gobiernos de los países adherentes a las Directrices

de la OCDE, en cooperación con las empresas y partes interesadas, con intervención de la Agencia de Acceso a la Información Pública en las cuestiones que hacen a su competencia para favorecer la fluidez de los mecanismos para el ejercicio de derechos.

Por otra parte, la creación de un Consejo para la transparencia en la AAIP que trabaje diariamente focalizado al establecimiento de criterios para la tutela efectiva, ejercicio de derechos, auditorías externas, recepción de consultas específicas de empresas cuando sus tratamientos generen riesgos residuales, como así también foco de asistencia a usuarios y capacitaciones para concientización.

Será necesario avanzar cuanto antes en la creación de mecanismos más aceitados de colaboración, concientización y rendición de cuentas, para enfrentar los múltiples riesgos en derechos fundamentales que estas innovaciones indefectiblemente ya están generando, a veces con más ruido y otras, más en silencio.

BIBLIOGRAFÍA

ABC (2013). Los resultados de búsqueda en Google reflejan prejuicios raciales. https://www.abc.es/medios-redes/20130204/abci-google-201302041645.html

Agencia de Acceso a la Información Pública y Autoridad Reguladora de Uruguay (2020) https://www.argentina.gob.ar/sites/default/files/guia_final.pdf

Agencia Española de Protección de Datos Personales (2021). Gestión del riesgo y evaluación de impacto en tratamientos de datos personales.

Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa (2018). Manual de legislación europea en materia de protección de datos.

Agrawal, A., Gans, J. S., & Goldfarb, A. (2019). Artificial intelligence: the ambiguous labor market impact of automating prediction. Journal of Economic Perspectives, 33(2), 31-50.

Ali, M., Sapiezynski, P., Bogen, M., Korolova, A., Mislove, A., & Rieke, A. (2019). Discrimination through optimization: How Facebook's Ad delivery can lead to biased outcomes. Proceedings of the ACM on Human-Computer Interaction, 3(CSCW), 1-30.

Apple (2021). User Privacy and Data Use. https://developer.apple.com/app-store/user-privacy-and-data-use/

Apple (2021). Un día en la vida de tus datos. https://www.apple.com/la/privacy/docs/A_Day_in_the_Life_of_Your_Data.pdf

Arthur, W. B. (1995). Complexity in economic and financial markets. Complexity, 1(1), 20-25.

Barforoush, A., Shirazi, H., & Emami, H. (2017). A new classification framework to evaluate the entity profiling on the web: Past, present and future. ACM Computing Surveys (CSUR), 50(3), 1-39.

Barrett, C. (2020). Emerging Trends from the First Year of EU GDPR Enforcement. Scitech Lawyer, 16(3), 22-35.

BBC Mundo Tecnología (2015). Google pide perdón por confundir a una pareja negra con gorilas.

https://www.bbc.com/mundo/noticias/2015/07/150702_tecnologia_google_perdon_confundir_afroamericanos_gorilas_lv#:~:text=%22Consternado%22.,su%20software%20de%20inteligencia%20artificial.

BBC News Mundo (2019). Cambridge Analytica: la multa récord que deberá pagar Facebook por la forma en que manejó los datos de 87 millones de usuarios https://www.bbc.com/mundo/noticias-49093124

Bertoni, E (2021). Introducción. Guía de privacidad para América Latina. International Association of Privacy Professionals (2021).

Cámara Federal de Mendoza, sala B, 24/05/2019, AR/JUR/12577/2019. Fallo P. A. E. c. Facebook Argentina SRL s/ medida autosatisfactiva.

Chatfield, T. (2012). Cosas que hay que saber sobre mundo digital.

Comité de Ministros del Consejo Europeo (2020). Impactos de los sistemas algorítmicos en los derechos humanos.

Comité Europeo de Protección de Datos (2021). El EDPB y el SEPD piden la prohibición del uso de IA para el reconocimiento automático de características humanas en espacios de acceso público y algunos otros usos de la IA que pueden conducir a una discriminación injustahttps://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en

Consejo Europeo (2017). Grupo de Trabajo del Artículo 29 sobre Decisiones automatizadas y perfilados.

Corvalán, J. G. (2020). Inteligencia artificial desde una perspectiva de desarrollo asimétrico. Diario Constitucional y Derechos Humanos Nro. 253.

Damia, J.M. (2010). Meta Analitycs.

Davenport, T. H., Barth, P., & Bean, R. (2012). How big data'is different.

David I. (2021). YouTube reinstates channels devoted to exposing conservative extremism. NBC News.

de Desarrollo, B. I. (2020). La Inteligencia artificial al Servicio del Bien Social en América Latina y el Caribe. Panorámica Regional e Instantáneas de Doce Países.

de Datos, R. I. D. P. (2017). Estándares de protección de datos personales para los Estados Iberoamericanos. México, Infoem.

Dirección Nacional de Protección de Datos Personales (2016). Debate público sobre necesidad de reforma Ley 25.326. https://www.argentina.gob.ar/sites/default/files/documento_aportes_reforma_ley25326_0.pdf

Edwards, L., & Veale, M. (2017). Slave to the algorithm: Why a right to an explanation is probably not the remedy you are looking for Duke L. & Tech. Rev., 16, 18.

Europea, U (2013). Dictamen del Consejo Europeo sobre las aplicaciones de los dispositivos inteligentes y publicidad del comportamiento en línea.

Europea, U. (2016). Reglamento 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales ya la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE

Europea, U. (2017). Directrices sobre la evaluación de impacto relativa a la protección de datos y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679.

Europea, U. (2017). Directrices sobre transparencia en virtud del Reglamento 2016/679.

Europea, U (2018). Directrices relativas al ámbito territorial del Reglamento 2016/679.

Europea, U. (2020). Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza. Oficina de Publicaciones de la Unión Europea.

Ezrachi, A., & Stucke, M. E. (2016). The rise of behavioural discrimination.

Goodman, B., & Flaxman, S. (2017). European Union regulations on algorithmic decision-making and a “right to explanation”. AI magazine, 38(3), 50-57.

Granero, H. R. (2019). Un futuro de participación entre humanos y algoritmos inteligentes. In *El derecho de las TIC en Iberoamérica* (pp. 1133-1141). La Ley (Uruguay).

Hao K. (2019). El algoritmo de publicación de anuncios de Facebook discrimina por género y raza**.** MIT Technology Review. https://www.technologyreview.com/2019/04/05/1175/facebook-algorithm-discriminates-ai-bias/

Harwell, D. (2021). Meet the scientist teaching AI to police human speech. The Washington Post.

India today (2021). Google le dice al Panel de TI del Parlamento que sus empleados escuchan algunas consultas de Ok Google.

Iproud (2021). Sundar Pichai: el CEO de Google opina sobre los cambios que trajo la pandemia, y mucho más. https://www.iproup.com/innovacion/23266-ceo-de-google-opina-sobre-lo-que-cambio-con-la-pandemia

Kaminski, M. E., & Malgieri, G. (2019). Algorithmic impact assessments under the GDPR: producing multi-layered explanations. U of Colorado Law Legal Studies Research Paper, (19-28).

Kartajaya, H., Kotler, P., & Hooi, D. H. (2019). Marketing 4.0: moving from traditional to digital. World Scientific Book Chapters, 99-123.

Li, Y. (2021). Didi shares drop on report China is planning unprecedented penalties https://www.cnbc.com/2021/07/22/didi-shares-drop-on-report-china-is-planning-unprecedented-penalties.html

Martínez, S. F. (2020). Las líneas directrices de la OCDE para las empresas multinacionales y su puesta en práctica por los puntos nacionales de contacto. Lex Social: Revista de Derechos Sociales, 10(2), 101-129.

Metcalf, J., & Crawford, K. (2016). Where are human subjects in big data research? The emerging ethics divide. Big Data & Society, 3(1), 2053951716650211.

Miazzo, C., Bilbao, A., & Bernardi, A. (2008). La rendición de cuentas de sostenibilidad de las empresas radicadas en América del Sur. Revista de Gestão Social e Ambiental, 2(3), 59-77.

OCDE (2013). Exploring the Economics of Personal Data: A survey of Methodologies for Measuring Monetary Value», OECD Digital Economy Papers, n.o 220, OECD Publishing, París, http://dx.doi.org/10.1787/5k486qtxldmq-en

OCDE (2011). Líneas Directrices de la OCDE para Empresas Multinacionales. https://www.oecd.org/daf/inv/mne/MNEguidelinesESPANOL.pdf

One Trust Hamburgo (2021), HmbBfDI emite una decisión que inicia un procedimiento administrativo contra Clearview AI Inc.

Palazzi, P. (2021). Argentina. Guía de privacidad para América Latina. International Association of Privacy Professionals (2021).

Peppers, D., Rogers, M., & Dorf, B. (1999). Is your company ready for one-to-one marketing. Harvard business review, 77(1), 151-160.

Peruzotti, M. (2021). Alcance territorial de las Leyes de Protección de Datos Personales. Diario La Ley.

Red Iberoamericana de Protección de Datos Personales (2017). Estándares Iberoamericanos

Red Iberoamericana de Protección de Datos (2019). Recomendaciones generales para el tratamiento de inteligencia artificial.

Rifkin, J. (2014). La sociedad de coste marginal cero. Barcelona: Paidós.

Roig, A. (2020). Las garantías frente a las decisiones automatizadas: del Reglamento General de Protección de Datos a la gobernanza algorítmica. Las garantías frente a las decisiones automatizadas, 1-276.

Russell, S., & Norvig, P. (2002). Artificial intelligence: a modern approach.

The technolawgist (2019) RGPD: análisis del primer año.
https://www.thetechnolawgist.com/2019/05/24/rgpd-analisis-del-primer/

Segura, P. (2021). Guía de privacidad para América Latina. International Association of Privacy Professionals (2021).

Thurm, S., & Kane, Y. I. (2010). Your apps are watching you. The Wall Street Journal, 17(1).

Winer, R. S. (2001). A framework for customer relationship management. California management review, 43(4), 89-105.

Zhou, N. (2021). Google engañó "parcialmente" a los consumidores sobre la recopilación de datos de ubicación, según un tribunal australiano. Diario The Guardian.