Maestría en Gestión de Servicios Tecnológicos y de Telecomunicaciones

Tutora: Mitchelstein, Eugenia

Tema:
Impacto del Reglamento General de Protección de Datos (GDPR) en las empresas con modelo de negocio de monetización de datos.

Alumno: Heffes, Guido

Buenos Aires, Argentina
2022

Índice

1. Introducción

1.1 Presentación del tema

La temática en este trabajo de investigación es el modelo de negocio de monetización de los datos, y el impacto del Reglamento General de Protección de Datos (GDPR).

El GDPR es un reglamento que entró en vigencia en Europa en Mayo de 2018, con el objetivo de mejorar la preservación de los datos personales de los individuos dentro de la Unión Europea, dándoles a éstos mayor control sobre los mismos. El GDPR aplica a los controladores y procesadores de datos, incluso si éstos se encuentran fuera de la UE, en los casos en que traten datos pertenecientes a residentes de la UE.

Un aspecto importante que introduce el GDPR es el derecho a la portabilidad de datos (art. 20). En el mismo se establecen determinadas situaciones en las cuales el interesado puede solicitar la devolución o transferencia de sus datos personales entre distintos responsables.

La monetización de datos implica descubrir y aprovechar el potencial de los datos de una empresa para obtener oportunidades, beneficios e ingresos. En muchas ocasiones es el principal activo de una compañía, el cual puede incluir un modelo de negocios orientado a la venta de los datos a otras empresas, o la usabilidad de los mismos.

1.2 Problemática y justificación del tema

En este trabajo de investigación se profundizará en las nuevas consideraciones que introduce el GDPR, y cómo éstas afectan a las empresas que incluyen, dentro de sus modelos de negocio la monetización de datos. La consideración de datos personales bajo GDPR es mucho más amplia de lo que era bajo reglamentaciones anteriores. Por ejemplo, las direcciones IP, información cultural, mental o económica, son bajo GDPR, considerados datos personales.

Se buscarán ejemplos de empresas que operaban previamente a la entrada en vigencia del nuevo reglamento europeo, y se analizará cómo éstas están enfrentando los desafíos y cambios que implica, y también las nuevas oportunidades que se generan. Se analizará el ejemplo de las grandes empresas líderes en el manejo y monetización de datos como Facebook, Twitter, Microsoft y

Google, así como también ejemplos de start ups o empresas pequeñas.

La principal problemática encontrada y que me ayudó a querer profundizar en el tema es la falta de preparación general de las empresas al GDPR, a pesar de que hubo 2 años para adaptarse, ya que entró en vigor en 2016, y su año de aplicación fue en 2018.

El uso ilegal de datos de Facebook que afectó a cerca de 87 millones de usuarios, hizo que Mark Zuckerberg se haya convertido en un gran embajador del GDPR. Tanto desde Facebook como desde otras compañías como Microsoft, han afirmado que aplicarán las nuevas normas y principios básicos para todos los usuarios, sin importar si son residentes de la UE o no. En este sentido, Facebook, Twitter, Microsoft y Google, se han unido en un proyecto denominado Data Transfer Project, el cual se encuentra en fase de desarrollo, y les permitirá a los usuarios trasferir fácilmente sus datos entre los distintos servicios de dichas empresas.

A pesar de estas acciones, existen sanciones importantes a raíz del GDPR. Una de las primeras multas relacionadas con la aplicación del GDPR fue cuando la CNIL (Comisión Nacional de Informática y Libertades), la agencia de protección de datos francesa, multó a Google LLC en 50 millones de euros por incumplimiento de las reglas del GDPR acerca de la transparencia y de la ausencia de una base legal válida de procesamiento de los datos personales destinados a fines publicitarios. Al poco tiempo, British Airways fue sancionada con más de 213 millones de euros. En el presente trabajo se investigarán las sanciones por GDPR, y la evolución de las mismas desde la entrada en vigor de la ley.

Las soluciones que están desarrollando las diferentes organizaciones son bastante variadas, pero está claro que el GDPR ha tenido efectos masivos en los negocios que implicaban datos de una u otra forma para sobrevivir. También puede verse que muchas empresas parecen haber dejado todo para el último momento, a pesar de haber tenido dos años para adaptarse.

Un nuevo reglamento es considerado necesario, dados los avances tecnológicos, la Directiva de Protección de Datos no era suficientemente efectiva para proteger los derechos de los usuarios respecto a su información personal. Colateralmente, startups pequeñas parecen haberse visto perjudicadas, al no contar con los suficientes recursos para adaptarse al nuevo reglamento, ayudando a reforzar el dominio de grandes corporaciones que tienen más recursos para la adaptación sin perder ventajas competitivas.

Definitivamente el GDPR representa un cambio cultural, generando nuevos procesos o modificaciones en los mismos por parte de las organizaciones, así como también nuevos riesgos. Al mismo tiempo, presenta oportunidades para ganar nuevamente la confianza de los usuarios, a partir de políticas de uso de datos responsables y que cumplan con el GDPR, y poder utilizar el nuevo escenario como un nuevo modo de diferenciarse.

El cumplimiento del GDPR puede ser solo el comienzo. A pesar de que el proceso de cambio se pueda estar dando lentamente, el mismo se está dando. Las estrategias de datos ofensivas y defensivas tienen el potencial de interrumpir y transformar la forma en que los consumidores comparten sus datos con las empresas, y qué es lo que deben hacer las empresas para mantener y profundizar la información de sus clientes, mientras intentan cumplir con el GDPR.

Es importante entender si el management piensa en cómo usar el GDPR para atacar a rivales e incluso a empresas fuera de su propia industria. Por ejemplo, una compañía de servicios financieros que obtiene el permiso del consumidor para solicitar sus datos a una compañía de tecnología, o viceversa. Pero al hacer esto se necesitará una carga significativamente mayor para las capacidades de datos de una empresa típica, lo que hará que los jefes de datos y equipos de ingeniería de datos experimentados, que ya escasean, tengan una demanda aún mayor, y sean un claro lugar de asignación de esfuerzos en la actualidad y los próximos años.

1.3 Preguntas

¿Cuáles son los cambios que trae el GDPR respecto al manejo de los datos personales y su impacto en las empresas con modelo de monetización de datos? ¿El impacto es global o se delimita a la UE?

¿Cómo se adaptan empresas grandes y pequeñas al GDPR? ¿Afecta su competitividad?

1.4 Objetivos

-Identificar los impactos que el GDPR genera en las empresas que siguen un modelo de negocio de monetización de datos.

-Investigar cómo el GDPR impacta tanto en las grandes empresas líderes, como en start ups o pequeñas empresas que monetizan los datos.

-Evaluar y comprender cuál es el impacto del GDPR en cuanto a sanciones por incumplimiento de la ley, las sanciones que se han dado, y sus motivos.

1.5 Hipótesis

El GDPR tiene un impacto global que no se delimita solamente a la UE. A su vez, las empresas más pequeñas tienen mayores dificultades para adaptarse al GDPR que los gigantes tecnológicos. El GDPR genera grandes esfuerzos en los gigantes tecnológicos por adaptarse y no quedar fuera de cumplimiento, y al mismo tiempo, pequeñas empresas que utilizaban modelos de monetización de datos, ya han desaparecido o lo van a hacer en el corto plazo.

2. Metodología de la investigación

2.1 Paradigma

El paradigma que se utiliza en este trabajo de investigación final es de forma complementaria, tanto el cualitativo como el cuantitativo.
Se presentan apreciaciones subjetivas así como también datos sólidos y concretos provenientes de estadísticas que brinden un sustento a conclusiones formuladas. El que predomina en nuestro caso va a ser el cualitativo.
Cook y Reichardt (1986) resaltan como ventajas del uso del paradigma cuantitativo y cualitativo el estudio de objetivos múltiples, puntos de vista e informaciones que ninguno de los dos paradigmas por separado podría brindar y la contrastación de resultados.

2.2 Tipo de investigación

La investigación fue predominantemente explicativa porque intenta responder las causas de los sucesos estudiados, va más allá de la descripción de los conceptos e intenta explicar por qué ocurren. Es por eso que se intenta explicar por qué ocurre lo descripto y la correlación de las variables con los hechos que se dan en el trabajo. Es ahí que la investigación presenta el carácter descriptivo, ya que se analiza el presente de la problemática a partir de opiniones, puntos de vista y actitudes con una buscada profundidad. La investigación no presenta la minuciosidad necesaria para calificarla meramente descriptiva, y también se busca dar con las razones o causas de los hechos descriptos.

2.3 Instrumentos

Los instrumentos que se utilizaron fueron predominantemente las entrevistas. A partir de una buena cantidad de información obtenida, que presenta la situación del GDPR y su impacto en las empresas de tecnología y que monetizan datos, en el trabajo de campo, se buscaron las opiniones de expertos que coincidan o no con los datos seleccionados.

Realicé una entrevista a Luis Blanco, que es especialista en Data Protection y Seguridad de la Información, y en el momento de la entrevista ocupaba el cargo de Gerente de Seguridad de la Información de AT&T International.

Al mismo tiempo, con el objetivo de tener un punto de vista orientado al ámbito legal y el GDPR, entrevisté a Manuela Mizraje, que es abogada y actualmente vive en México, y se desempeña como Gerente de Ética y Compliance en Reckitt México, y también a Valentina Salas, que es abogada de Baker Mckenzie en Argentina, y especialista en Data Protection.

Por otro lado, realicé una entrevista a Germán Rosón, que ocupa el cargo de Country Manager para Panamá y El Salvador. El objetivo de esta entrevista fue tener el punto de vista del liderazgo de grandes empresas, y así ampliar la visión por fuera de especialistas en Data Protection.

También, analicé videos relacionados con los gigantes tecnológicos que operan en la UE y cómo han enfrentado el GDPR, su impacto luego de la implementación, y papers y publicaciones con datos relevantes respecto a multas y sanciones. Además, analicé los casos de las empresas SKY Brasil y AT&T, y cómo éstas se vieron afectadas por el GDPR.

2.4. Triangulación

Entrevistas a Luis Blanco, Manuela Mizraje, Germán Rosón y Valentina Salas

Análisis de datos y videos relativos al impacto del GDPR y su implementación

Casos de empresas (AT&T y SKY Brasil), y otras pequeñas empresas que monetizan datos

Figura 1. Triangulación. Fuente: Elaboración propia.

Cook y Reichardt (1986) enumeran las ventajas de la triangulación:

1. Posibilita la atención a los objetivos múltiples que pueden darse en una misma investigación.
2. Se vigorizan mutuamente brindando puntos de vista y percepciones que ninguno de los dos podría ofrecer por separado.
3. Contrastando resultados posiblemente divergentes y obligando a replanteamientos o razonamientos depurados.

2.5 Cuadro de Variables de Investigación

VARIABLES	DIMENSIONES	INDICADORES	INSTRUMENTOS
GDPR y sus nuevas consideraciones respecto a datos personales	Consideraciones respecto a los datos personales	Cantidad de tipos de datos considerados como datos personales antes y después del GDPR	Entrevistas, análisis de datos
	Nuevas implicancias generadas por el GDPR y la portabilidad de datos	Nivel de adecuación/cumplimiento promedio de las empresas previo a la implementación del GDPR	Entrevistas, análisis de datos
Impacto en las empresas de tecnología que monetizan datos	Preparación de las empresas a la entrada en vigor del GDPR	Nivel de adecuación/cumplimiento promedio de las empresas luego de la implementación del GDPR. Sanciones aplicadas	Entrevistas, análisis de datos
	Impacto económico negativo del GDPR en empresas que monetizan datos	Cantidad de empresas de tecnología que monetizan datos y tuvieron que cerrar.	Entrevistas, análisis de datos
	Impacto económico positivo de la llegada del GDPR	Nuevas oportunidades de negocio generadas con el GDPR	Entrevistas, análisis de datos

Figura 2. Cuadro metodológico. Fuente: Elaboración propia.

3. Marco Teórico

3.1 Reglamento General de Protección de Datos (GDPR)

El GDPR es un reglamento que entró en vigencia en Europa en Mayo de 2018, con el objetivo de mejorar la preservación de los datos personales de los individuos dentro de la Unión Europea, dándoles a éstos mayor control sobre los mismos. El GDPR aplica a los controladores y procesadores de datos, incluso si éstos se encuentran fuera de la UE, en los casos en que traten datos pertenecientes a residentes de la UE. Dicho reglamento sustituye la Directiva de Protección de Datos, o Directiva 95/46 / CE, y dispone una armonización de los reglamentos de protección de datos en toda la UE (Greengard, 2018).

Vanberg (2018) amplía en que el texto final del GDPR se acordó en el diálogo tripartito entre el Consejo Europeo, el Parlamento y la Comisión el 15 de diciembre de 2015 y se publicó el 4 de mayo de 2016 en el Diario Oficial de la Unión Europea. Después de dos años de período de transición, el GDPR es vinculante para todos los estados miembros a partir del 25 de mayo de 2018.

El impacto del GDPR es analizado por Greengard (2018): "GDPR permite a los consumidores eliminarse de una base de datos o fuente en línea en cualquier momento; las compañías que violan GDPR enfrentan multas de hasta el 4% de sus ingresos anuales globales. Por encima de todo, GDPR representa la batalla en curso entre el capitalismo sin restricciones y la dignidad humana."

Knack, Cohen y McAllister (2018) explican que el GDPR impone varios requisitos nuevos y aumenta las sanciones por incumplimiento. Un enfoque principal del GDPR ha sido relativo al incumplimiento, que son considerables. Las violaciones pueden resultar en multas de hasta el mayor de € 20,000,000 o 4 por ciento de los ingresos anuales de una compañía.

Además, estos mismos, en relación a los límites de aplicación del GDPR, desarrollan que la pregunta clave es si se están procesando datos personales de los residentes de la UE. Un franquiciador puede procesar datos personales de residentes de la UE cuando califica a los franquiciados, como parte programas de fidelización de clientes, y para otros fines. Franquiciadores comprometidos en publicidad dirigida y seguimiento de individuos en línea que son residentes de la UE como así cualquier intercambio de información personal entre franquiciadores y los franquiciados activarán el cumplimiento.

O'Connor (2017) desarrolla que el objetivo del GDPR es armonizar las leyes de privacidad de datos en toda Europa y crear un campo de juego nivelado. El mismo trae cambios significativos en la forma en que las empresas deben manejar y procesar información personal. Los procesos existentes de las organizaciones, que pueden incluir recopilación, retención y eliminación, entrada general, etc., deben revisarse para que cumplan plenamente con las nuevas reglas de protección de datos, que son más estrictas que nunca. El GDPR puede verse como una oportunidad fantástica para ordenar sus datos, reconectarse con sus clientes y construir relaciones mejores y más sólidas.

Además de ser responsables de su propia recopilación y procesamiento de datos, también se espera que las organizaciones se aseguren de que los proveedores externos, cumplan con las disposiciones del GDPR independientemente de la ubicación geográfica. Esta responsabilidad se describe claramente en el artículo 44, que permite la transferencia de datos personales solo si el controlador y el procesador cumplen las condiciones establecidas en la ley, incluidas las transferencias posteriores de datos personales desde el tercer país o un país internacional a una organización de otro tercer país u otra organización internacional (Sanders, 2019).

Buenadicha Sánchez, Galdon, Hermosilla, Loewe y Pombo (2019) enumeran los principios básicos que trae el GDPR relativo al manejo de los datos personales:

"(i) deben ser tratados de forma lícita, leal y transparente; (ii) se deben recolectar con fines determinados explícitos y legítimos; (iii) deben ser adecuados, pertinentes y limitados a lo necesario dependiendo del uso; (iv) deben ser exactos y estar siempre actualizados; (v) deben mantenerse de forma tal que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento; y (vi) deben ser tratados de tal manera que se garantice su seguridad."

3.2 Privacidad

Buenadicha Sánchez, Galdon, Hermosilla, Loewe y Pombo (2019) resumen la privacidad de los datos y los riesgos a los que se enfrentan las empresas con la entrada en vigor del GDPR: "El primer riesgo (y el más evidente) al que se enfrentan quienes manejan datos personales es el de la protección de estos y, en un sentido más amplio, el de la privacidad. En realidad, es precisamente esta última la que ha producido un mayor número de referencias y marcos jurídicos, no solo por el hecho de que se trata de un derecho reconocido en muchas constituciones nacionales, sino

especialmente debido a la expedición y entrada en vigor en 2018 del Reglamento General de Protección de Datos (RGPD) de la Unión Europea, que en poco tiempo se ha convertido en una suerte de estándar de referencia global (CNIL, S.f.).”

A su vez, argumentan que uno de los efectos positivos de una gestión responsable de los datos es que esta se traduce de forma automática en una mayor seguridad de tal información y de los sistemas que la almacenan. Los cortafuegos, el cifrado, la anonimización y la codificación son algunas de las modalidades de protección de los datos personales, tanto en los programas como en los equipos informáticos. Aun así, el acceso ilegal o piratería (hacking) es habitual, y cuando la información no está anonimizada, el impacto de estos robos es tan significativo que el GDPR obliga a divulgar públicamente estos hechos. Igualmente prevé multas multimillonarias para aquellos casos en que los responsables de los datos no hayan tomado medidas de seguridad y anonimización acordes con los riesgos existentes.

3.3 Portabilidad de datos

El derecho a la portabilidad de datos les permite a los usuarios a llevarse fotos, contactos, mails, en caso de que cambien de compañía.

Vanberg (2018) desarrolla sobre el derecho de la portabilidad de datos en el GDPR requerirá que las empresas se aseguren de que pueden entregar los datos personales proporcionados por un individuo en un formato utilizable y transferible. El preámbulo del GDPR demuestra que el derecho a la portabilidad de los datos se aplicará a la computación en la nube, los servicios web, los sistemas de teléfonos inteligentes y otros sistemas automatizados de procesamiento de datos. El derecho a la portabilidad de los datos se aplicará a una amplia gama de áreas, como las redes sociales, medios, buscadores, almacenamiento de fotos, correo electrónico y tiendas online. Será igualmente aplicable a bancos, compañías farmacéuticas, proveedores de energía, aerolíneas, incluso a pequeñas empresas como pizzerías o sastres si son controladores de datos y se ocupan de datos personales.

Quinn (2018) destaca un concepto importante que trae la portabilidad de datos relacionado con los datos alcanzados por el GDPR: “Otra advertencia importante que debe considerarse de la portabilidad de datos como lo describe el GDPR es que se aplica solo a los datos personales

proporcionados por el sujeto de los datos. Esto se puede dividir en dos requisitos separados (i) que los datos sean de naturaleza personal y (ii) que sean proporcionados por el interesado."

Ambos autores, realizan buenas descripciones de los conceptos que trae la portabilidad de datos, y a quienes aplica, pero no realizan un análisis de posibles impactos del mismo, ni de qué es lo que deberán hacer las empresas para enfrentar el el proceso de adaptación.

A su vez, según O'Connor (2017), los interesados también tendrán derecho a la portabilidad de los datos (es decir, la capacidad de obtener y reutilizar sus datos personales para sus propios fines en diferentes servicios) y, si requieren más información sobre sus datos, las organizaciones deben facilitar la solicitud de dichos datos y proporcionar una respuesta integral dentro de un mes a partir de la fecha de solicitud. Todo esto conducirá inevitablemente a un aumento importante de la carga administrativa para las organizaciones, y esa carga será particularmente onerosa para aquellas empresas que almacenan datos en papel.

3.4 Protección de datos personales

Es importante entender qué datos son alcanzados por la reglamentación, y a qué nos referimos cuando hablamos de datos personales y su protección. En este sentido, Buenadicha Sánchez, Galdon, Hermosilla, Loewe y Pombo, (2019) desarrollan este concepto indicando que no se limita a nombres y apellidos, sino que además incorpora cualquier elemento que pueda llevar a la identificación de un sujeto determinado. Así, los identificadores únicos de computadores y teléfonos, como también los datos geolocalizados y los biométricos, constituyen datos personales y deben quedar sujetos a protección legal incluso cuando no se encuentran directamente asociados a un nombre propio. Si se busca compartirlos o abrirlos, será necesario definir un protocolo robusto de anonimización o seudonimización para evitar su mal uso o su empleo con fines distintos a los expresados cuando se los recolectó en una primera instancia. Es importante insistir en que la anonimización deberá ser robusta, pues, aunque una base de datos haya sido anonimizada, su cruce con otras puede derivar en la reidentificación de algunos individuos.

Según O'Connor (2017), un sujeto de datos es la persona viva con quien se relacionan los datos personales. Bajo GDPR, los interesados tendrán mucho más control sobre sus datos personales y, de manera bastante significativa, el derecho a ser olvidados. Esto significa el borrado completo de

sus datos personales. Los procesos de gobernanza interna de las organizaciones ahora deberían revisarse y, muy probablemente, modificarse antes de la fecha de implementación del GDPR. Se aplicarán nuevas obligaciones de gobernanza de datos y entrarán en vigor los registros de cómo deben preparar y mantener los registros de las actividades de procesamiento.

Sanders (2019) detalla que el GDPR define los datos personales de manera mucho más amplia de lo que normalmente se define en las leyes existentes, donde la legislación específica del sector generalmente se centra en la información que puede identificar directamente a una persona.

Además, agrega que bajo el GDPR, los interesados tienen una serie de derechos que las organizaciones deben respetar, como el derecho a acceder a sus datos (artículo 15), el derecho a corregir sus datos (artículo 16), y el derecho a borrado (artículo 17).

3.5 GDPR en Argentina

La modificación normativa en materia de datos personales realizada en la Unión Europea consistente en la sanción del Reglamento General de Protección de Datos (o más conocido como GDPR por sus siglas en inglés General Data Protection Regulation) trascendió la frontera de la Unión Europea. Y ello se debe no solamente a la extraterritorialidad que el propio GDPR establece, sino a la influencia en estados como Argentina, considerados por la Unión Europea como país con protección adecuada en materia de datos personales, que continuando la tendencia van camino a armonizar su normativa y estándares a los nuevos lineamientos sentados por el GDPR.

Así, desde la sanción del GDPR, Argentina comenzó un proceso de actualización del régimen de datos personales. Entre dicho proceso se puede mencionar la adhesión al Convenio 108, el hecho de que se encuentra bajo tratamiento por el Congreso de la Nación un proyecto de modificación de la actual Ley N° 25.326 de Protección de Datos Personales (la "LPDP") y la emisión de nueva reglamentación por parte de la Agencia de Acceso a la Información Pública (la "AAIP").

3.6 GDPR en México

El caso de México está muy bien explicado por Pérez Gómez (2021): "México, basándose en los principios de la Directiva de la UE, publicó el 5 de julio de 2010, la Ley Federal de Protección de

Datos Personales en Posesión de los Particulares, y posteriormente, su regulación secundaria (la "Ley de Datos"). La Ley de Datos no ha sido homologada al GDPR; sin embargo, las personas y sociedades mexicanas podrían estar obligadas a cumplir con el GDPR en caso de que (i) ofrezcan y entreguen productos o servicios de manera habitual a habitantes de la UE, o (ii) utilicen herramientas que les permitan rastrear cookies o direcciones IP de personas que visiten su sitio web desde países de la UE."

A su vez, agrega que la Ley de Datos y el GDPR comparten principios sustancialmente iguales, pero que hay determinadas obligaciones que incorporó el GDPR, que no están previstas aún en la regulación mexicana:

-El derecho a la portabilidad, el cual faculta al titular a obtener una copia de sus datos personales tratados por el responsable;

-Introduce el principio de protección de datos desde el diseño (Privacy by Design);

-Establece obligaciones expresas respecto del consentimiento de un niño menor a 16 años; y

-Obligaciones y requisitos nuevos en caso de que el responsable utilice tecnologías novedosas en el tratamiento de datos.

Además sugiere que las Entidades mexicanas que puedan obtener y tratar datos de residentes de la UE o las subsidiarias mexicanas de empresas internacionales, deben analizar el impacto del GDPR en sus operaciones en México, y considerar fortalecer su régimen de protección de datos personales, para cumplir con los estándares internacionales, incluyendo el GDPR, para evitar contingencias y multas.

3.7 GDPR en Brasil

En Brasil, la ley de protección de datos es la Lei Geral de Proteção de Dados Pessoais, que significa "ley general de protección de datos personales". La Lei Geral de Proteção de Dados se redactó tomando como modelo el GDPR europeo, y crea un marco legal sobre cómo se permite administrar los datos personales en Brasil. Contiene sesenta y cinco artículos.

La LGPD entró en vigor en agosto de 2020 con un periodo de gracia de 12 meses. Su aplicación comenzó en agosto de 2021 y está dirigida por la Autoridad Nacional de Protección de Datos (ANPD).

Koch (2019) marca sobre el artículo 18 que es otra sección de la LGPD que les resultará familiar a las empresas que se han ocupado del cumplimiento del GDPR. Explica los nueve derechos fundamentales que tienen los interesados, entre los que se encuentran:

-El derecho a la confirmación de la existencia del tratamiento;

-El derecho a acceder a los datos;

-Derecho a rectificar datos incompletos, inexactos o no actualizados;

-El derecho a anonimizar, bloquear o eliminar datos innecesarios o excesivos o datos que no estén siendo procesados de conformidad con la LGPD;

-Derecho a la portabilidad de los datos a otro proveedor de servicios o productos, mediante solicitud expresa

-El derecho a eliminar los datos personales tratados con el consentimiento del interesado;

-El derecho a la información sobre las entidades públicas y privadas con las que el responsable haya compartido datos;

-El derecho a la información sobre la posibilidad de denegar el consentimiento y las consecuencias de tal denegación; y

-El derecho a revocar el consentimiento.

A pesar de sus objetivos similares y la aparente influencia que tuvo el GDPR en los legisladores brasileños, hay algunas diferencias clave a tener en cuenta entre las dos leyes (Koch , 2019).

-Oficiales de protección de datos: ambos actos requieren que las empresas y organizaciones contraten a un Oficial de Protección de Datos (DPO). Sin embargo, mientras que el GDPR establece cuándo se requiere un DPO, el artículo 41 de la LGPD simplemente dice: "El controlador designará a un oficial para que esté a cargo del procesamiento de datos", lo que sugiere que cualquier organización que procese los datos de personas en Brasil necesitará contratar un DPO.

Esta es otra área que probablemente recibirá más aclaraciones, pero tal como está escrito, es una de las pocas áreas en las que la LGPD es más estricta que el GDPR.

-Base legal para el procesamiento de datos: posiblemente, la diferencia más significativa entre la LGPD y el GDPR tiene que ver con lo que califica como base legal para el procesamiento de datos. El GDPR tiene seis bases legales para el procesamiento, y un controlador de datos debe elegir una de ellas como justificación para usar la información de un interesado. Sin embargo, en el artículo 7, la LGPD enumera 10.

-Reportar violaciones de datos: el GDPR es explícito: una organización debe informar una violación de datos dentro de las 72 horas posteriores a su descubrimiento. La LGPD no da ningún plazo en firme.

-Multas: las multas bajo la LGPD son mucho menos severas. El artículo 52 establece que la multa máxima por infracción es "2% de los ingresos de una persona jurídica privada, grupo o conglomerado en Brasil, durante el ejercicio fiscal anterior, sin impuestos, hasta un máximo total de 50 millones de reales" (esto funciona aproximadamente 11 millones de euros). Las multas de LGPD están en línea con las multas de GDPR por infracciones menos graves, pero 11 millones de euros no afectarán a los procesadores de datos más grandes del mundo.

3.8 Competitividad

Porter (1985) señala que la competitividad es la capacidad de una empresa para producir y mercadear productos en mejores condiciones de precio, calidad y oportunidad que sus rivales.

Según Ivancevich y Lorenzi (1997), la competitividad es la medida en que una nación, bajo condiciones de mercado libre y leal, es capaz de producir bienes y servicios que puedan superar con éxito la prueba de los mercados internacionales, manteniendo y aún aumentando al mismo tiempo, la renta real de sus ciudadanos.

Adam Smith fue quien presentó el primer argumento moderno sobre la competitividad, al cuestionar la idea mercantilista de que el secreto de la superioridad de un país estaba en el control de la economía y la maximización de sus reservas en oro y plata. Smith celebraba los beneficios

de la competencia para lograr la maximización de la eficiencia y como consecuencia mejorar el bienestar.

En este sentido, según Apleyard y Field (2003) Smith centró sus ideas sobre la actividad económica dentro de un país a la especialización y el intercambio entre países. Afirmó que los países deberían especializarse y exportar aquellos bienes en los cuales tuvieran una ventaja absoluta y deberían importar aquellos bienes en los cuales el socio comercial tuviera una ventaja absoluta. Cada país debería exportar aquellos bienes que produjera más eficientemente porque el trabajo absoluto requerido por unidad era menor que aquel del posible socio comercial.

Porter (1990) concluye que en un número cada vez mayor de industrias, la ventaja competitiva proviene de factores (como el conocimiento y la pericia) que se crean y no se heredan. Los factores más importantes en muchas industrias son aquellos cuyo desarrollo requiere una inversión pública y privada significativa, y aquéllos empleados en una o pocas industrias. Estos factores promueven las ventajas, ya que tienden a ser difíciles de imitar o de obtener a distancia. En algunos casos, las desventajas en factores básicos pueden servir de estímulo a la innovación y, en última instancia, crean ventajas. Sin embargo, dichas desventajas deben ser selectivas, más que sistémicas, para promover innovación y ventajas.

Estudiando las cinco fuerzas competitivas, Porter (1997) explica que la intensidad de la competencia en un sector industrial no es ni coincidencia ni mala suerte. Más bien, la competencia en un sector industrial tiene sus raíces en su estructura económica fundamental y va más allá del comportamiento de los competidores actuales. La situación de la competencia en un sector industrial depende de cinco fuerzas competitivas básicos:

-La rivalidad entre los competidores existentes en el sector industrial.

-La amenaza de productos o servicios sustitutos.

-La amenaza de nuevos ingresos en el sector.

-El Poder negociador de los clientes.

-El Poder negociador de los proveedores.

La acción conjunta de estas fuerzas determina la rentabilidad potencial en el sector industrial, en donde el potencial de utilidades, de beneficios se mide en términos del rendimiento a largo plazo del capital invertido. No todos los sectores industriales tienen el mismo potencial; se distinguen

fundamentalmente en el potencial de utilidades finales a medida que difiere la acción conjunta de dichas fuerzas, que pueden variar desde intensas hasta relativamente débiles. Lógicamente, en aquellos sectores donde la competencia es intensa, ninguna empresa obtendrá rendimientos espectaculares, mientras que en los sectores en los que la competencia es débil, son bastante comunes los rendimientos elevados.

Estas cinco fuerzas competitivas reflejan el hecho de que la competencia en un sector industrial va más allá de los simples competidores. los clientes, proveedores, sustitutos y competidores potenciales son todos competidores para las empresas en un sector industrial y pueden ser de mayor o menor importancia, dependiendo de las circunstancias particulares. La competencia, en un sentido más amplio, podría denominarse rivalidad amplificada.

Las cinco fuerzas competitivas conjuntamente determinan la intensidad competitiva así como la rentabilidad del sector industrial, y la fuerza o fuerzas más poderosas son las que gobiernan y resultan cruciales desde el punto de vista de la formulación de la estrategia. Por ejemplo, incluso una empresa con una posición fuerte en el mercado en un sector industrial en donde los competidores potenciales no constituyen una amenaza, obtendrá bajos rendimientos si se enfrenta a un sustituto superior, de coste más bajo. Aun si no existen sustitutos y está bloqueado el ingreso, la intensa rivalidad entre los competidores existentes limitará los rendimientos potenciales. El caso extremo de "intensidad competitiva" en un sector industrial está representado por la competencia perfecta de los economistas, en donde el ingreso es libre, las empresas existentes no tienen poder negociador con los proveedores y los clientes, y la rivalidad es desenfrenada debido a que las numerosas empresas y los productos son todos similares (Porter, 1997).

3.9 Modelo de negocio

Con el objetivo de entender posibles impactos del GDPR en los modelos de negocios de monetización de datos, es necesario primero ahondar en los conceptos de Osterwalder, Pigneur y Tucci (2005), que definen modelo de negocio: “Un modelo de negocio es una herramienta conceptual que contiene un conjunto de elementos y sus relaciones y permite expresar la lógica de negocios de una empresa específica. Es una descripción del valor que una empresa ofrece a uno o varios segmentos de clientes y de la arquitectura de la empresa y su red de socios para crear,

comercializar y entregar este valor y capital de relación, para generar flujos de ingresos rentables y sostenibles."

En este mencionado paper, se hace una búsqueda de los orígenes del concepto, y cuando empezó a utilizarse. Para esto, los autores han realizados una gran búsqueda bibliográfica de manera electrónica: "Sorprendentemente, la investigación muestra que la popularidad del término "modelo de negocio" es un fenómeno relativamente joven. Aunque apareció por primera vez en un artículo académico en 1957 [Bellman, Clark, et al. 1957] y en el título y el resumen de un artículo en 1960 [Jones 1960], se destacó recién hasta fines de los años noventa. Este aumento de coincidencias coincide con el advenimiento de Internet en el mundo de los negocios y el pronunciado aumento del índice de la bolsa de valores NASDAQ para empresas de tecnología pesada. El término se usó con mayor frecuencia, pero no solo en relación con Internet a partir de la década de 1990 en adelante."

3.10 Monetización de datos

La monetización de datos se refiere a descubrir y aprovechar el potencial de los datos de una empresa para obtener oportunidades, beneficios e ingresos extra, u otras veces, es el principal activo de una compañía, el cual puede incluir un modelo de negocios orientado a la venta de los datos a otras empresas, o la usabilidad de los mismos. Se refiere al uso de los mismos para adquirir un beneficio económico que pueda ser cuantificable. Dentro de esto, podemos considerar métodos como el intercambio y venta de información a terceros, o el desarrollo de nuevos productos y servicios que se basen en el análisis de esos datos que determinada compañía posee (Monetización de datos: la estrategia más rentable de analytics, 2016).

Desde el punto de vista tecnológico, la inteligencia artificial, machine learning, cloud computing y hadoop, entre otras, son tecnologías o nuevos desarrollos por los cuales se le facilita a las organizaciones el procesamiento masivo de datos en tiempo real, así como la integración de datos. Hay condiciones que facilitan la monetización, tales como: costos de almacenamiento de datos mínimos, mayor disponibilidad y accesibilidad a los datos, y los retornos de las inversiones en Big Data y Analytics (¿Qué es el big data?, s.f.).

Sutton (2018) en Data for Dollars, se focaliza en los nuevos modelos de negocio que se han generado en relación a los datos personales, pero no explica ni investiga las empresas que quedan en el camino y/o no logran adaptarse a la nueva normativa para subsistir. Dentro de esto, destaca que algunos servicios se están adelantando a la curva regulatoria al ofrecer a los consumidores la oportunidad de rastrear sus datos en un lugar y tomar decisiones sobre cómo se usan sus datos y a quiénes se proporcionan. Estos servicios ofrecen una plataforma móvil central en la que los consumidores pueden cargar datos personales y realizar acuerdos de intercambio de datos individuales con las entidades de su elección.

Además, se puede destacar que las empresas toman cada vez más decisiones a través de los datos, y toman decisiones sobre los datos que son propiedad del consumidor; sin embargo, el consumidor no entiende qué es esa información, cómo se está utilizando o el valor general que está creando, dijo Neil Sweeney, fundador y CEO de Killi, una aplicación que permite a los consumidores compartir datos personales, como direcciones de correo electrónico, ubicación e identificadores móviles con compradores de datos a cambio de efectivo. Neil Agrega que las compañías están ganando miles de millones y miles de millones de dólares, y el consumidor cotidiano no obtiene nada a cambio (Sutton, K., 2018).

O'Connor (2017) plantea que el período de preparación de GDPR es un buen momento para revisar sus datos, no solo con el propósito de cumplir con el GDPR, sino también por razones de desarrollo comercial. Pueden las organizaciones preguntarse si realmente conocen a sus clientes, si pueden ayudar a mejorar la relación con ellos, para que pueda satisfacer mejor sus necesidades mientras protege la información que le han proporcionado. El consentimiento y el uso general de los datos personales deben evaluarse sin importar qué. Dicho esto, puede convertir este requisito en una fuerza para el bien y generar una confianza mucho mayor con sus clientes y empleados en el proceso.

Según Astrid Bohé (2013), la monetización de datos no es un descubrimiento nuevo, desde siempre, las organizaciones han tratado de aprovechar la información en pos de realizar más y mejores negocios. Lo que ha ido cambiando son los modelos de negocio, dependiendo de las innovaciones que se van sucediendo.

En ese sentido agrega que analizar y emplear los datos de los clientes no es nuevo. Las fuentes tradicionales de datos se han utilizado para mejorar el rendimiento de las ventas y el marketing

desde que se produjo y distribuyó el primer catálogo de pedidos por correo hace más de dos siglos. Desde informes de ventas mensuales hasta inteligencia comercial predictiva, aprovechar los datos de los clientes es una forma bien conocida de mejorar la eficiencia, construir relaciones con los clientes y generar nuevos ingresos.

Por último, concluye que la evolución de las redes de comunicación, el incremento en la penetración de internet, la velocidad con que los nuevos desarrollos tecnológicos se suceden, las capacidades de tratamiento de grandes volúmenes de información, todo eso genera el ambiente de negocio propicio para la proliferación de modelos de negocio de monetización de datos de maneras que hasta hace muy poco tiempo no hubiésemos imaginado.

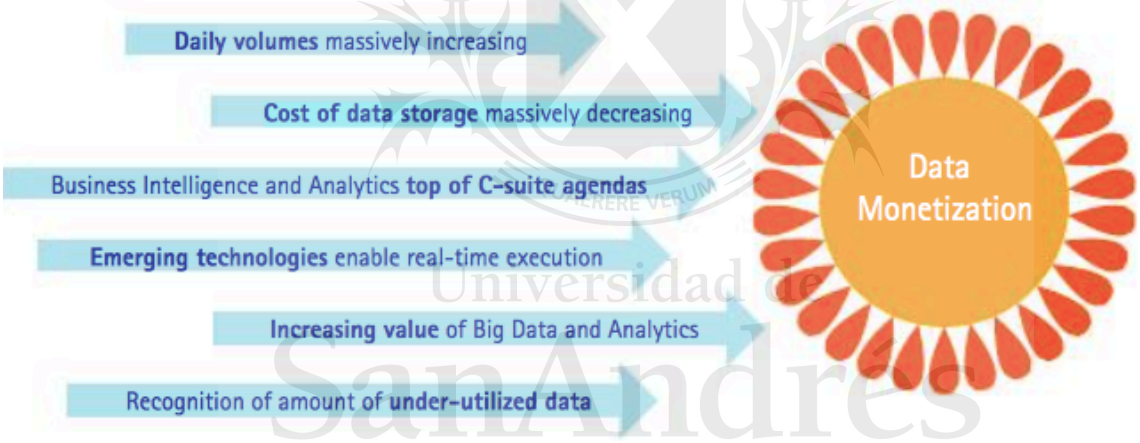

Figura 3. Fuerzas que empujan la Monetización de Datos (Astrid Bohé, 2013).

Gal y Aviv (2020), explican que los datos constituyen un insumo importante en las operaciones de una empresa, y por ende se debe elegir una estrategia para recopilar y procesar dichos datos. Con base en entrevistas con participantes del mercado, identifican cinco estrategias principales empleadas por los actores del mercado para acumular datos relevantes:

1. Recopilación de datos orgánicos (datos de primera mano): la empresa recopila los datos directamente del Sujeto de datos.

2. Fusionarse con una entidad y usar sus datos en sus propias operaciones.

3. Comprar o recibir los datos de un proveedor externo (datos de terceros). Esta opción también incluye el intercambio de datos mediante el uso de una interfaz de programación de aplicaciones (API). Una API es una interfaz o protocolo de comunicación entre un cliente y un servidor de modo que el servidor iniciará una acción definida, incluida la provisión de datos, en respuesta a una solicitud reconocida por parte del cliente de datos en un formato específico.

4. Convertirse en parte de una empresa conjunta en la que las empresas agrupan sus datos (o conocimiento basado en datos) para fines específicos predefinidos.

5. Comprar/recibir conocimiento basado en datos (en lugar de datos), o datos agregados, de un proveedor externo (agente de conocimiento). Por ejemplo, Google ofrece un servicio que utiliza su base de datos para responder consultas sin exponer los datos que sirvieron de base para las respuestas. De manera similar, los servicios de conocimiento del mercado brindan informes sobre las tendencias de mercado. Esta opción no está sujeta al GDPR.

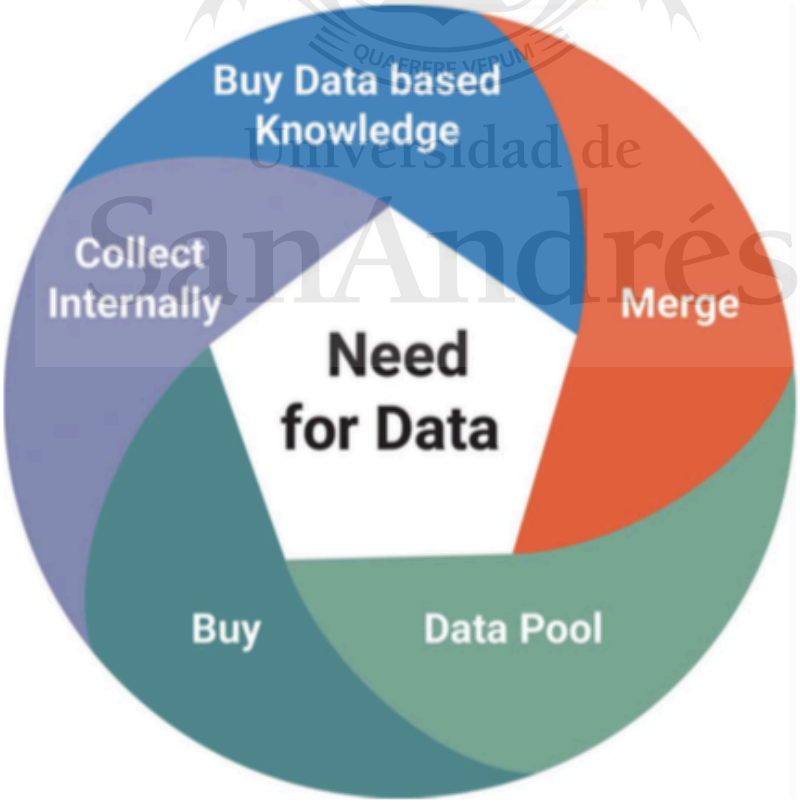

Figura 4. Cinco opciones para obtener los datos necesarios o el conocimiento basado en datos (Gal y Aviv, 2020).

Las empresas eligen entre estas opciones en función de su rentabilidad relativa, así como de su viabilidad y escalabilidad, que, a su vez, se ven afectadas por una combinación de barreras tecnológicas, financieras, estratégicas y legales.

3.11 Paradigma digital

Las tecnologías digitales han cambiado al mundo en la forma en que se piensa acerca de los datos. Los datos eran costosos de obtener y difícil de almacenar. La gestión de los datos requiere de eficientes sistemas de IT para su mantenimiento. Actualmente, la generación de datos se encuentra a un ritmo sin precedente. Por otro lado, los sistemas en Cloud para el almacenamiento de datos son cada vez más baratos y eficientes. El mayor desafío de la actualidad es convertir los datos en información valiosa (Rogers, 2016).

Respecto a la accesibilidad, almacenamiento y disponibilidad de la información, es fundamental destacar la influencia y el desarrollo de las tecnologías en la nube. A pesar de ser un modelo de almacenamiento de datos ideado en los años 60, en los cuales los espacios de almacenamiento están virtualizados, en la última década ha habido un crecimiento exponencial del uso de estos servicios, tanto para el usuario final como para las empresas y organizaciones que van a ser las que tengan los datos de estos usuarios.

El mejor ejemplo de esto es Amazon Web Services, lanzado en 2006, creció masivamente y ganó dominación del mercado ofreciendo servicios como networking, storage, database, analytics and deployment. Para 2015 ya servía a 1 millón de clientes activos en 190 países, incluyendo agencias gubernamentales, start ups, instituciones educacionales y organizaciones sin fines de lucro, siendo la división más rentable de Amazon. Dos fenómenos a analizar respecto a esto: 1) años atrás, empresas tradicionales de cierta envergadura, preferían comprar hardware para alojar las aplicaciones, datos y plataformas. Hoy en día la tendencia a la utilización de la nube ha crecido enormemente, en tiempos donde la conectividad permite un mejor funcionamiento de dichas tecnologías, con menores inversiones, y menos staff de mantenimiento y soporte. 2) el fácil acceso

de usuarios finales o empresas más pequeñas a este tipo de tecnologías, hace mucho más frecuente el almacenamiento, accesibilidad, disponibilidad y capacidad monetización de esos datos para este tipo de empresas (Young Koo, 2017).

La nube puede reducir el costo de propiedad de equipos, aplicaciones y personas para dar mantenimiento y ejecutar las aplicaciones. Para una empresa común, el Cloud reduce drásticamente los gastos para los mismos servicios. Esto puede dar lugar a un ahorro entre 20 a 50% en costos con tecnología.

Según Kozlowski (2017), desde una perspectiva tecnológica, la clave para el éxito de una solución en la nube es la capacidad de hiperescala. La hiperescala define una arquitectura que puede ampliarse adecuadamente a medida que crece la demanda. Las soluciones hiperescalables ya suponen 20% del mercado de centros de datos y son cada vez más generalizadas.

Big Data es un término referido al gran volumen de datos, ya sean estructurados o no estructurados. Son conjuntos de datos o combinaciones cuyo tamaño, complejidad y velocidad de crecimiento dificultan su captura, gestión, procesamiento o análisis mediante tecnologías y herramientas convencionales. Lo importante respecto al Big Data es lo que las organizaciones hagan con los datos, es decir, el análisis que se haga sobre esos datos, con el objetivo de obtener ideas para mejores decisiones estratégicas de negocio. Este análisis ayuda a las organizaciones a sacar provecho de sus datos y utilizarlos para identificar nuevas oportunidades, movimientos de negocio más inteligentes, mayores ganancias y clientes satisfechos. Una de las formas de sacar valor con el Big Data que tienen las empresas es la reducción de costos con la utilización de tecnologías de datos ya mencionadas como Hadoop, y análisis en la nube. De esta manera, con estas tecnologías más veloces, se agiliza la toma de decisiones, y se pueden desarrollar y lanzar nuevos productos y servicios, a partir de una medición de las necesidades de los clientes y su satisfacción mediante el análisis de los datos (Big Data: ¿En qué consiste? Su importancia, desafíos y gobernabilidad, s.f.).

Según Santamarta, Gandhi, & Bechauf, (2019), el desafío de big data es hacer uso de los datos de manera consciente. Un estudio de BCG encontró que la reacción de los clientes al mal uso de los datos puede hacer que reduzcan en un tercio sus gastos en una empresa. Los líderes en big data generan alrededor de 12% más de ingresos que los que no aprovechan al máximo la analítica.

4. Trabajo de Campo

Se estudiaron los casos de dos empresas grandes que no tienen presencia en la Unión Europea, y se analizó cómo se han visto afectadas por el GDPR de manera directa o indirecta, ya sea por leyes locales relacionadas con el GDPR o por lo que generó el GDPR como nuevo estándar en cuanto al manejo de los datos personales. Además, se buscaron casos de empresas pequeñas que monetizan datos, y se analizaron los impactos del GDPR en las mismas.

Por otro lado, las cuatro entrevistas realizadas muestran distintos puntos de vista vinculados con los impactos que trae el GDPR en las empresas, de manera coincidente o no, y relacionados con la globalidad, y diferencia en cuanto a la magnitud de la empresa en cuestión. Lo importante en la selección de los entrevistados fue encontrar, por un lado, expertos en Data Protection con diferentes antecedentes o especialidades, como Luis Blanco, vinculado con la tecnología y los sistemas y seguridad de la información, y Valentina Salas, con lo legal. Una de las entrevistas es a un directivo de una empresa tecnológica como Germán Rosón, y por último, Manuela Mizraje que también es abogada, se desempeña en Compliance y tiene conocimientos relativos al manejo de los datos pero no es espcecialista en Data Protection como Valentina.

A su vez, se analizaron videos relacionados con los gigantes tecnológicos que operan en la UE y cómo han enfrentado el GDPR, su impacto luego de la implementación, y papers y publicaciones con datos relevantes respecto a multas y sanciones.

4.1 Caso AT&T

AT&T, Inc. es un conglomerado de empresas y sociedad multinacional estadounidense con sede en Dallas, Texas. Es la compañía de telecomunicaciones más grande del mundo, el mayor proveedor de servicios de teléfono móvil y el proveedor más grande de servicios de teléfono fijo en los Estados Unidos a través de AT&T Communications. Desde el 14 de junio de 2018, también es la empresa matriz del conglomerado de medios de comunicación WarnerMedia (anteriormente TimeWarner), lo que la convierte en una de las compañías de entretenimiento y medios más grande del mundo. A partir de 2018, AT&T ocupa el puesto # 9 en la clasificación Fortune 500 de las corporaciones más grandes de los Estados Unidos por el ingreso total.

En el 2016 adquirió DirecTV, transformando AT&T uno de los mayores operadores de televisión por satélite en los Estados Unidos y América Latina.

AT&T se presentaba antes de la entrada en vigor del GDPR de la siguiente manera: "AT&T tiene un compromiso de larga data para proteger los datos del cliente, y esto incluye cumplir con el GDPR. Actualmente estamos modificando el lenguaje de la guía de servicios y contratos para abordar los requisitos reglamentarios. Planeamos responder rápidamente a las solicitudes de acceso de los interesados, consultas de las autoridades europeas de protección de datos y notificaciones de violaciones de la privacidad de datos."

AT&T destaca que los siguientes derechos de privacidad están incluidos en el reglamento:

- Notificaciones de incumplimiento: las empresas deben notificar a los clientes dentro de las 72 horas de haberse enterado de una violación de datos.
- Derecho de acceso: las personas tienen derecho a saber si sus datos personales se están procesando, dónde se procesan y con qué propósito.
- Derecho a ser olvidado: las personas tienen derecho a que una empresa borre sus datos personales, deje de difundirlos más y, posiblemente, que terceros detengan el procesamiento de los datos.

También se incluyen los siguientes requisitos organizativos:

- Mayor alcance territorial: el GDPR se aplicará al procesamiento de datos personales por parte de los controladores y procesadores en la UE, independientemente de si el procesamiento se lleva a cabo en la UE o no.
- Oficial de protección de datos (DPO): su organización puede requerir el nombramiento de un Oficial de protección de datos (DPO).
- Privacidad por diseño: las empresas solo pueden conservar y procesar los datos de un individuo cuando sea absolutamente necesario para completar sus funciones.

En línea con estos puntos, AT&T estableció una serie de políticas, y determinó un equipo responsable por el enforcement y capacitación respecto al GDPR (DPO), además de los equipos de legales y privacidad de los datos que trabajan en conjunto todos estos temas. Las siguientes son algunas de las políticas que AT&T hace aplicables a todas sus subsidiarias:

- Privacy by Design

- EU GDPR Incident Management
- EU e-Privacy Directive
- EU Privacy Incident
- AT&T Business Customer GDPR Privacy Notice
- Data Subject Access Rights
- EU Data Subject Access Rights Management
- EEA Consent Management
- EEA Privacy Data Lifecycle
- EU Data Subject Access Rights Management
- EU Lawfull Basis of Processing
- Export of EEA Personal Data
- Management of Privacy Policy and Notices
- Privacy Incident Management
- Privacy Regulatory Compliance
- Reporting Privacy Related Incidents

Como bien mencioné anteriormente, AT&T es una de las compañías más importantes y grandes del mundo, y a pesar de que sus principales negocios y empresas subsidiarias se encuentran fuera de Europa, ha hecho todos estos esfuerzos para ser compliance con el GDPR.

4.2 Caso SKY Brasil

SKY es el mayor operador de TV paga vía satélite del Brasil. Desde su apertura en 1996, distribuye programación 100% digital a sus suscriptores en todo el territorio nacional. Tiene más de 5,3 millones de clientes, que representan poco más del 28% de todos los suscriptores de TV paga en Brasil.

Desde sus inicios, SKY siempre ha sido pionera en el lanzamiento de una serie de novedades e innovaciones tecnológicas en la televisión paga en Brasil, combinadas con programación para los diversos perfiles de clientes y excelencia en el servicio. Fue la primera en lanzar los recursos que transformaron la TV, trayendo al país servicios inéditos como transmisiones de cine en pantalla ancha (pantalla rectangular, 16 por 9), uso de multicámaras para mostrar concursos y espectáculos,

Televisión Mejorada (programas de información en pantalla adicional y juegos), el primer DVR (SKY+), y el primer servicio de video bajo demanda, "Cine SKY HD" y el primer modelo de TV paga prepago del mercado nacional.

En febrero de 2017, SKY lanzó el satélite SKY B1, que puede operar con hasta 60 transpondedores de 36 MHz en la banda Ku, y asegurará la ampliación de la cantidad de canales ofrecidos por SKY, reafirmando el ADN del operador de ofrecer productos y servicios innovadores, anticipándose a las tendencias del mercado e invirtiendo en tecnología e infraestructura.

En orden de no quedar fuera de compliance con el LGPD, en 2019 SKY Brasil firmó un contrato con K2View en el cual adquiere el desarrollo e implementación de su solución para GDPR, así como el licenciamiento por 5 años. Dicho contrato tiene un costo aproximado de un 1,2M USD y tiene posibilidad de renovación luego del vencimiento en 2024.

La solución de K2View para el cumplimiento de GDPR y CCPA también es compatible con las normas específicas impuestas por CPRA, CDPA, LGPD, PDPA y POPIA. De hecho, es flexible para adaptarse a las nuevas regulaciones de privacidad de datos con simples cambios de configuración. Se conecta a los datos del cliente, sin importar dónde residan, y los mapea en una Digital Entity que representa a cada cliente. Con un solo click, ofrece una respuesta segura y automatizada a cualquier solicitud de datos de un sujeto, con características que abordan necesidades críticas de privacidad de datos. La solución K2View recopila datos de todas las fuentes subyacentes, automáticamente, para permitir el cumplimiento de DSAR en solo unos minutos. También permite la eliminación de los datos de un cliente de todos los sistemas, en caso de que se ejerza el "derecho al olvido".

El software de cumplimiento de K2View GDPR y CCPA aborda todos los aspectos de la privacidad de datos, incluido:

-Punto único para el consentimiento: lo que hace que sea simple y claro para los clientes optar por aceptar o no y limitar los tipos de recopilación de datos.

-Derecho de acceso seguro: mantener el acceso a los datos de un cliente no importa cuántos sistemas y bases de datos pueda estar disperse.

-Portabilidad de datos: permite que el cliente lleve rápida y fácilmente sus datos personales (y su negocio) a otro lugar.

-Derecho a ser olvidado: permite a los clientes controlar cuánto tiempo puede almacenar y usar sus datos, después de lo cual debe eliminarlos.

-Protección de datos: proporciona seguridad que limita el acceso a las personas autorizadas y limita la exposición potencial y las violaciones de datos.

-Informes de violaciones: notifica a los clientes de manera oportuna si su información personal está en riesgo debido a una violación.

4.3 Casos de empresas pequeñas

Algunas empresas de datos directamente no pudieron adaptarse a la nueva reglamentación impuesta por el GDPR. Un ejemplo es Klout, que fue un sitio web y una aplicación móvil que usó el análisis de redes sociales para calificar a sus usuarios de acuerdo con la influencia social en línea a través del "Klout Score", que es un valor numérico entre 1 y 100. Klout llegó a alcanzar una gran importancia en el mundo de los community managers, relaciones públicas, influencers y demás personal relacionado con el marketing y ventas. Era una especie de medidor de reputación basado en la presencia y popularidad en diferentes medios. Unos años después de ser adquirido por Lithium Technologies por 200 millones de dólares, y teniendo la intención de realizar una IPO para salir a oferta pública, cosa que finalmente no sucedió, la empresa anunció su cierre. Esto sucedió paralelamente a la incorporación del Reglamento General de Protección de Datos. Lithium especificaba que utilizaba la información personal de los usuarios para sus propios intereses legítimos y los de sus socios comerciales. Esta situación con el GDPR como una de sus causas, se puede entender que se convirtió en insostenible.

Otras empresas similares han optado por bloquear el tráfico de los países de la Unión Europea, para de esta manera evitar sanciones por incumplimiento del GDPR. En línea con esto, Brent Ozar Limited, una academia que brindaba clases en línea y en vivo para aprender sobre servidores SQL, ha dejado de operar en la UE. Brent Ozar, el director del sitio, afirma que es un gran admirador de la ley, y que las empresas que usan tus datos personales sin obtener su consentimiento personal deberían cerrar. Por otro lado agrega que: “Somos una pequeña empresa con sede en los Estados Unidos. No pensarías que sería un gran problema, pero te sorprenderías. Por ejemplo, los estudiantes nos envían información sobre sus bases de datos todo el tiempo como parte de sus

preguntas y, a menudo, la envían sin que la soliciten, a través de canales de correo electrónico no cifrados. Esa información termina por todos lados: nuestros servidores de correo, nuestras computadoras de escritorio, teléfonos, computadoras portátiles, índices de búsqueda, etc. Realmente no me preocupa que mantengamos la confidencialidad de esos datos, pero ahora tendríamos que agregar nuevo seguimiento auditable" (Ozar, 2021).

Según el GDPR, si alguien nos pide que eliminemos sus datos, no solo tenemos que eliminarlos, sino que debemos auditar que los eliminamos y mantener esos registros para las autoridades de la UE. Y luego responder a las solicitudes de la UE para esa documentación concluye Brent.

"Creemos que pocas entidades cumplen al 100% pero la mayoría han dado pasos importantes para un cumplimiento total. Especialmente las grandes empresas han dado pasos decididos en cuanto al cumplimiento; las pequeñas empresas están en general menos concientizadas", asegura Juan Jesús Merino Torres, National Channel Country Manager de BitDefender (Pérez, 2018).

La opinión es compartida por Ignacio Gilart, CEO de WhiteBearSolutions, afirma que "si bien es cierto que las medianas y grandes organizaciones han cumplido en su gran mayoría con la adaptación, muchas pequeñas organizaciones no han cumplido ni son conscientes del impacto de no hacerlo" (Gilart, 2017).

Otro buen ejemplo es Streetlend. Christian Beach, su creador desarrolla: "Streetlend era un sitio web que ayudaba a vecinos y amigos a prestar elementos entre ellos. Escaleras, taladros, etc. Llegamos a tener cientos de artículos, principalmente en Londres. Se realizaron muchas transacciones sin fricción y sin cargo para el prestamista o el prestatario en nuestros 5 años de operación".

Con la llegada del GDPR Christian entiende que: "La ley, combinada con firmas legales parásitas sin ánimo de lucro, pone a los propietarios de sitios web en riesgo de denuncias vengativas. Los sitios web y las organizaciones sin ánimo de lucro jóvenes no pueden pagar los equipos legales. Por lo tanto, el riesgo planteado por el GDPR es inaceptablemente alto". De hecho, este empresario tiene una interpretación muy particular respecto a la intención de la ley:

"Perversamente, esta nueva ley perjudica especialmente a las startups pequeñas y éticas, y ayuda a reforzar el dominio de las grandes corporaciones, porque estas pueden prepararse y defenderse usando equipos legales establecidos y reservas de efectivo" (Pérez, 2018).

4.4 Hallazgos de las entrevistas

4.4.1 Principales impactos del GDPR

Luis y Valentina coinciden en que hay 2 principales impactos que trae el GDPR en las empresas: la problemática que trae al momento de cumplir con la reglamentación, y el otro impacto es directamente costo. El hecho de tener que invertir en recursos y equipos dedicados a desarrollar políticas internas y enforzar su cumplimiento dentro de las organizaciones es un punto importante a considerar. El no cumplimiento puede traer publicidad negativa, damnificando la reputación de la empresa y penalidades monetarias, así como riesgos legales. Las multas llegan hasta 20 millones de euros y/o el 4% del revenue.

Estos 2 puntos podrían ampliarse de la siguiente forma para los entrevistados:

a. Impacto en los procesos: lleva a adoptar la privacidad desde el diseño. Es decir, repensar los procesos incorporando la perspectiva de la protección de datos desde el principio y como parte esencial de la vida de un proyecto (por ejemplo, haciendo evaluaciones de impacto de privacidad ("PIA", por sus siglas en inglés). Entre dichos procesos, se deberán incluir aquellos que permitan garantizar los derechos de los ciudadanos (no solo derechos ARCO pero también derechos como el de portabilidad, el cual es mucho más difícil de delimitar).

b. Impacto en los costos: Dar cumplimiento a dicho marco normativo implica alocar recursos de forma continua. No solo se trata de adaptar/crear procesos y estructuras/flujos de información que cumplan con el GDPR sino que el principio de "accountability" (no hay una traducción 100% precisa pero bien se acerca al concepto de "responsabilidad proactiva") obliga a que forme parte de las tareas del día a día. En otras palabras, no hay una fecha de "fin" o una "línea de llegada" sino que su cumplimiento es más bien un proceso constante y en movimiento; dinámico.

4.4.2 Globalidad o no del GDPR

Germán por otro lado menciona que el principal impacto del GDPR es el establecimiento de un nuevo estándar para el manejo de los datos personales por parte de las empresas, sin importar

exactamente donde esas empresas operen. Esa conciencia sobre el manejo de los datos es global, y se ha vuelto algo obligatorio en un contexto tan dinámico e interconectado.

Ampliando el punto de Germán, Manuela señala que el principal impacto que surgió con la aplicación del GDPR es que este aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión Europea (la "Unión"), independientemente de que el tratamiento tenga lugar o no en la Unión. A su vez, también explica que el tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:

-la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o

-el control de su comportamiento, en la medida en que este tenga lugar en la Unión.

Por tanto, el GDPR será aplicable cuando:

-la empresa trata datos personales y tiene su sede en la Unión, independientemente de dónde se traten de hecho los datos

-la empresa tiene su sede fuera de la Unión pero trata datos personales relativos a ofertas de bienes o servicios a ciudadanos en la Unión, o supervisa el comportamiento de ciudadanos en la Unión.

Germán y Manuela nos adelantan lo que Luis y Valentina coinciden en indicar. El impacto del GDPR es global, ya que si hay datos de cualquier ciudadano europeo que procese o almacene de cualquier empresa, dicha empresa debe tratar los mismos de acuerdo a lo que establece la ley europea. En grandes empresas, puede ocurrir que aplique la ley para algunas subsidiarias y para otras no, pero las mismas suelen implementarlo como buena práctica en todas sus subsidiarias, minimizando riesgos. El GDPR es de naturaleza expansiva y de aplicación extra-territorial.

4.4.3 Impacto del GDPR según la magnitud de la empresa

Respecto a la diferencia entre las grandes empresas con las medianas o pequeñas, Luis destaca que por supuesto que la ley aplica para todas, pero que por la capacidad de recursos a asignar de las grandes empresas, ya sea de legales, IT o consultorías especializadas externas, hay una desventaja

de las pequeñas y medianas empresas con respecto a las grandes, a la hora de implementar los procesos y controles necesarios para no quedar fuera de compliance con respecto al GDPR. A su vez, Valentina no hace una diferenciación entre grandes y pequeñas empresas, e indica que los esfuerzos varían de empresa a empresa.

Desde el punto de vista de la magnitud de la empresa, siempre que sea esta una empresa nacida o actualizada a la era digital, Germán no ve demasiadas diferencias en su aplicación y cumplimiento, más allá de que un esfuerzo siempre es necesario para no quedar fuera de compliance y estar sujeto a multas tan altas como establece el GDPR. Si bien las empresas pequeñas tienden a tener menor sustento y estructura como para poder enfrentar esos esfuerzos, las grandes tienen mayores riesgos en cuanto a las multas, ya que estas en general pueden tener que ver con porcentajes de ingresos de la misma empresa.

Por otra parte, Manuela destaca que si las empresas se manejan acorde a la legislación, el impacto en cuanto a cómo aplicar y qué aplicar debería ser similar en las empresas grandes que en las pequeñas. El problema, cuando se va a estudiar el impacto real del GDPR, es que las grandes compañías tienen una mayor estructura para hacer frente a estas obligaciones y un mayor presupuesto en caso de elegir tercerizar con especialistas el control y aplicación de la ley.

4.4.4 GDPR y el impacto en la competitividad

Analizando la competitividad de las empresas ante el GDPR, los cuatro coinciden en indicar que hay un claro impacto que trae el GDPR sobre las empresas. Manuela menciona que el GDPR se instaura como un nuevo elemento a tener en cuenta en la competitividad entre las empresas, y de no ser considerado por las mismas, se puede caer en fuertes multas y sanciones, lo cual en sí, es un factor de erosión de competitividad.

Luis afirma que la competitividad de las empresas que no cumplan se va a ver afectada, ya que los riesgos son grandes, pero por otro lado, realizar los esfuerzos necesarios para cumplir con el GDPR también es un factor de erosión de competitividad, ya que hay costos incrementales que antes de la ley no existían, ya sea por desarrollos en IT o por asignar equipos dedicados al control. Esa pérdida de competitividad por realizar los esfuerzos de ser compliance es menor que no cumplir y exponerse a multas y daños a la reputación de la empresa, y claramente representa un esfuerzo

mucho mayor para pequeñas y medianas empresas, que para las grandes. El ser GDPR compliance pasa a ser un factor de diferenciación.

Para Germán, la competitividad en el mercado global es cada vez más fuerte y compleja. Esto hace que muchos jugadores queden afuera del mercado sino se adaptan rápidamente a un entorno cambiante. El GDPR eleva la vara en cuanto al manejo de los datos y cómo las empresas deben manejarlos, esto hace que las empresas que no logren resolver estos temas, o no lo hagan de la manera más eficiente, queden al margen en esa competencia o sean relegados por las que sí puedan cumplir.

Valentina va más allá e indica que hay un impacto directo en la competitividad de las empresas. No solo a nivel de imagen o reputacional (el GDPR se volvió un estándar que da confianza a los titulares de datos/data subjects) sino que muchas empresas ven su cumplimiento como condición necesaria para contratar. En otras palabras, quien no cumple puede quedar fuera del mercado por exclusión de los otros actores que lo integran. Incluso tiene un impacto a nivel Estados. Los países que no realizan esfuerzos coordinados para, al menos, adecuarse a los estándares del GDPR no son vistos como países con legislación adecuada y esto afecta, entre otras cosas, la transferencia internacional de datos desde la UE a empresas ubicadas en dichos países. En un mundo globalizado donde los mercados están integrados y sus límites son difusos o, al menos, trascienden los límites geográficos de un país, el flujo de datos es clave. Esto ha sido un problema para Estados Unidos, país que no cuenta con una norma de protección de datos a nivel nacional y que no está dentro del listado de países con legislación adecuada de la UE. De hecho, en 2020 el último acuerdo -Privacy Shield- que permitía la transferencia de datos entre ambos bloques de forma legal fue anulado por el Tribunal de Justicia de la Unión Europea (TJUE).

4.4.5 Consideraciones adicionales

Valentina nos cuenta que recientemente, el 25 de marzo de 2022, se confirmó que la UE y Estados Unidos llegaron a un principio de acuerdo para desarrollar un nuevo marco jurídico que permita realizar transferencias transatlánticas de datos personales entre ambos bloques. El texto completo aun no fue publicado pero la Casa Blanca sí publicó un "Fact Sheet" que permite entrever algunos de los compromisos que Estados Unido se obliga a asumir.

Germán ve que el proceso de adecuación fue muy diferente en los distintos países del mundo, ya que no es la misma situación la de una empresa que opera directamente en la UE, que otra que no lo haga, por más que el impacto es global, lo que se puede ver es dicho impacto de estas nuevas normativas es de "cascadeo", es decir se va expandiendo, con distintas leyes locales basadas en el GDPR, o con buenas prácticas en cuanto al manejo de datos personales, sobre todo en empresas que operan globalmente.

Por otro lado, para Valentina el proceso de adecuación en general a la nueva normativa por parte de las empresas fue desafiante, intenso y complejo, y es un proceso que no ha acabado. No solo porque no todas las empresas se han adaptado (requiere muchos esfuerzos y recursos) sino porque aun aquellas que han iniciado el proceso deben seguir cumpliéndolo de forma constante. Ciertamente el GDPR no es sencillo y no existe un modelo de "one-size-fits-all" por lo que requiere un análisis pormenorizado y de caso a caso.

El otro elemento muy importante que introduce el GDPR para Manuela es la portabilidad de datos, permitiendo a los clientes, exigirle a las empresas la posibilidad de llevarse consigo todos sus datos personales cuando lo deseen. Esto a nivel global, es un cambio muy importante desde el punto de vista legal y pone a la empresas una presión extra a la hora del manejo de los datos de sus clientes.

4.5 Análisis de datos y videos

En el presente apartado, se analizaron los videos encontrados que se relacionan con los gigantes tecnológicos que operan en la UE y cómo han enfrentado el GDPR, su impacto luego de la implementación, y si han sufrido sanciones luego de la entrada en vigor. Además de esto, se estudiaron papers y publicaciones con datos relevantes respecto a cumplimiento del GDPR, multas y sanciones, así como también la competitividad de las empresas y cómo se ve afectada por el GDPR.

4.5.1 Análisis de videos y datos relacionados con los gigantes tecnológicos

En 2019, el regulador de protección de datos de Francia, CNIL, ha emitido a Google LLC una multa de 50 millones de euros por no cumplir con sus obligaciones de GDPR. Esta era la mayor

multa de GDPR hasta ese momento emitida por un regulador europeo y la primera vez que se descubre que uno de los gigantes tecnológicos no cumple con las nuevas y estrictas regulaciones que entraron en vigor en mayo de 2018.

CNIL dijo que la multa se emitió porque Google no pudo proporcionar suficiente información a los usuarios sobre sus políticas de consentimiento de datos y no les dio suficiente control sobre cómo se utiliza su información. Según el GDPR, las empresas deben obtener el "consentimiento genuino" del usuario antes de recopilar su información, lo que significa hacer que el consentimiento sea un proceso de aceptación explícito que las personas pueden retirar fácilmente.

En respuesta a la multa, un portavoz de Google dijo que la compañía está profundamente comprometida para cumplir con los altos estándares de transparencia y control que la gente espera de ella. Dijeron que la compañía estaba estudiando la decisión de CNIL para determinar sus próximos pasos. En una declaración posterior, Google anunció que planeaba apelar la multa, señalando que estaba preocupado por el impacto de esta decisión en los editores, creadores de contenido original y compañías tecnológicas en Europa y más allá.

En enero de 2022, Google pierde el recurso legal y no puede evitar una multa de 100 millones de euros impuesta por el CNIL. De esta manera el máximo tribunal francés respaldó a los reguladores.

Por separado, Google también ha sido acusado de violaciones de la privacidad GDPR por parte de grupos de consumidores en siete países europeos por lo que afirman que son "prácticas engañosas" en torno a su seguimiento de ubicación.

Facebook fue una de las líderes en implementar las políticas y procedimientos de tratamiento de datos que cumplan con el GDPR, como un estándar, sin importar donde aplica y a quienes. Esto se puede relacionar con al gran impacto que tuvo el escándalo de la filtración de datos de usuarios de Facebook por la empresa Cambridge Analytica en las elecciones presidenciales de Estados Unidos.

A pesar de esto, en 2021 la aplicación de mensajería instantánea WhatsApp fue sancionada por las autoridades irlandesas a pagar 225 millones de euros por violar la privacidad de los usuarios. WhatsApp Ireland Ltd es la empresa nacional que gestiona la aplicación en Europa, ha sido la compañía investigada. En respuesta a Irish Times, la comisaria de Protección de Datos Helen Dixon, explica que WhatsApp solo proporcionó a los usuarios el 41% de la información prescrita

a sus usuarios, pero ninguna a los no usuarios. Un "grave deficit de información" que se traduce en cuatro infracciones del GDPR, definidos por Dixon como "muy serios".

También en 2021, Amazon se enfrentó a la mayor multa de privacidad de la historia de la Unión Europea después de que su principal organismo de control de la privacidad le impusiera una sanción de 746 millones de euros por violar las estrictas normas de protección de datos del bloque. La CNPD, la autoridad de protección de datos de Luxemburgo, impuso a Amazon la multa récord en una decisión del 16 de julio de 2021 en la que acusó al minorista en línea de procesar datos personales en violación del GDPR.

Amazon en un comunicado afirma que no ha habido filtración de datos y ningún dato de cliente ha sido expuesto a ningún tercero, y agregó que planea apelar indicando que están totalmente en desacuerdo con el fallo de la CNPD.

La compañía dice que recopila datos para mejorar la experiencia del cliente y establece pautas que rigen lo que los empleados pueden hacer con ellos. Algunos legisladores y reguladores han expresado su preocupación de que la empresa haya utilizado lo que sabe para obtener una ventaja injusta en el mercado.

Microsoft se define con un gran compromiso hacia el responsable tratamiento de los datos y su implementación:

“Estamos comprometidos en asegurar que nuestros productos y servicios cumplen con el GDPR. Por eso, hemos contado con más de 1.600 ingenieros en la compañía trabajando en proyectos relacionados con el reglamento. Desde su entrada en vigor en 2016, hemos realizado importantes inversiones en rediseñar nuestras herramientas, sistemas y procesos para dar respuesta a los requisitos del GPDR. Hoy, su cumplimiento está fuertemente alineado con la cultura de Microsoft, e integrado en todos los procesos y prácticas que llevamos a cabo para crear y proporcionar productos y servicios.

Como regulación de la Unión Europea, el GDPR crea importantes nuevos derechos específicos para los individuos de la región. Sin embargo, creemos que esta regulación establece un importante principio que es relevante en todo el mundo.

Por eso, hoy queremos anunciar que vamos a ampliar todos los derechos que forman parte fundamental del GDPR a todos nuestros clientes en todo el mundo. Los Data Subject Rights,

incluyen el derecho a saber qué datos recopilamos, corregirlos, eliminarlos o incluso llevarlos a otra parte. Nuestro Panel de Privacidad ofrece a los usuarios las herramientas necesarias para tener el control de sus datos."

Además, dentro de su sitio web, estableció un centro de confianza, en donde están explicadas todas las buenas prácticas que trae el GDPR, y como estas impactan en los distintos productos de la empresa, así como facilidades para que cada usuario pueda administrar sus datos. Microsoft está utilizando al GDPR como un elemento de diferenciación.

4.5.2 Análisis de multas y sanciones por GDPR

Haraminac (2021), realiza un estudio sobre las multas bajo el GDPR. En la figura 5, se puede observar en dólares estadounidenses la suma de los importes de las multas agrupados por categorías antes de julio de 2019. La gran mayoría de estas multas (84 por ciento), se centraron en la seguridad de los datos, es decir acceso. Los datos no eran lo suficientemente seguros para evitar que personas no autorizadas, ya fueran internas o externas, accedieran a ellos. A medida que las organizaciones almacenan cantidades cada vez mayores de datos, aumenta el riesgo de un incidente de seguridad cibernética que involucre esos datos.

A su vez, las multas por procesamiento se imponen a las organizaciones que analizan, conectan o convierten datos de una manera que no se divulgó correctamente o para la cual la organización no obtuvo el consentimiento efectivo. Para evitar multas como estas, las organizaciones deben evaluar la realidad de sus propios datos almacenados. El almacenamiento es el hermano pequeño del acceso; Se han impuesto multas por almacenamiento a empresas que no eliminan datos de sistemas antiguos (como Morgan Stanley) o publican información personal en Internet cuando no deberían hacerlo, pero que no han sufrido una violación de datos perpetrada por un actor externo.

Se impusieron multas por uso a una empresa que envió millones de mensajes de marketing por correo electrónico a clientes sin el consentimiento de esos clientes para usar sus datos de esa manera. Otro ejemplo es una empresa que accedió a los datos de audio y GPS de los usuarios para detectar transmisiones no autorizadas de un evento deportivo (Haraminac, 2021).

Figura 5. Categorías de multas impuestas bajo GDPR antes de julio de 2019 (Haraminac, 2021).

Haraminac (2021) destaca que para el cierre de 2020, hay nueva información sobre las multas impuestas bajo GDPR, e indica una nueva dirección para la industria de protección de datos. La Figura 6 identifica dos nuevas categorías de multas impuestas hasta diciembre de 2020: recolección y política. Tres de las categorías originales (acceso, procesamiento y almacenamiento) aumentaron menos del 10 % desde mediados de 2019, mientras que las multas impuestas por el uso aumentaron un 87 %. Recolección es la categoría nueva más grande y consiste en multas impuestas a dos grandes empresas tecnológicas, Amazon y Google. Las multas de política son las que se imponen a las empresas con políticas deficientes en materia de protección de datos y prevención de la ciberseguridad, aunque no hayan sufrido una brecha interna o externa.

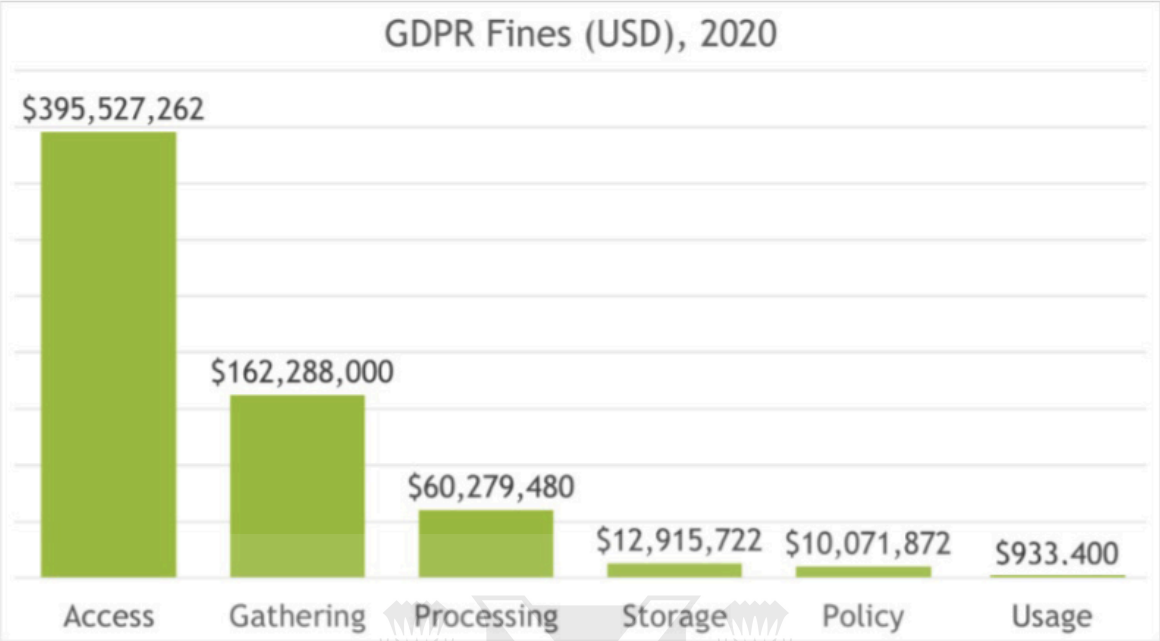

Figura 6. Categorías de multas impuestas bajo GDPR hasta diciembre de 2020 (Haraminac, 2021).

4.5.3 Análisis de competitividad y cumplimiento del GDPR

Por otro lado, el informe BCG/DLA Piper describe un proceso sencillo mediante el cual las empresas pueden pasar rápidamente del simple cumplimiento del GDPR al cumplimiento inteligente y, de allí, a la administración de datos confiable a los ojos de sus clientes. Y los beneficios de la confianza del consumidor pueden ser muy grandes: la investigación de BCG muestra que los consumidores tienen al menos cinco veces más probabilidades de compartir datos con una empresa en la que confían que con una en la que no (Baltassis, Rose y Gourevitch, 2018).

Gal y Aviv (2020), plantean en su estudio sobre los efectos competitivos del GDPR un escenario en el que el mismo puede generar ventajas para las empresas más grandes, reduciendo así la competencia potencial en el mercado. Esto se debe a varias razones. En primer lugar, las grandes empresas disfrutan de economías de escala y el alcance en la recopilación y gestión de datos que cumplen con el GDPR. Al reconocer este efecto, el GDPR impone requisitos más indulgentes a las pequeñas y medianas empresas.

Sin embargo, en algunas situaciones, esos estándares más bajos pueden perjudicar a dichas empresas en relación con los proveedores de datos que deben cumplir con los estándares más altos. Este puede ser el caso cuando la empresa A tiene la intención de integrar los datos de la empresa E con los suyos, creando un gran conjunto de datos que debe cumplir con los requisitos más estrictos. Por lo tanto, la empresa A puede preferir comprar datos que ya cumplen con los estándares más altos. Si el valor agregado para la Empresa A de adquirir dichos datos fuera significativo, una Empresa E pequeña o mediana podría optar voluntariamente por cumplir con los estándares más altos, renunciando así a la solución principal del GDPR sobre las desventajas competitivas que crea para las empresas pequeñas en relación con las grandes. Si los costos de cumplimiento fueran prohibitivos para las pequeñas empresas, el número e incluso la calidad de las fuentes de datos disponibles podrían reducirse.

Además, agregan que las limitaciones en el intercambio de datos pueden reducir la competencia y conducir a estructuras de mercado más concentradas. Aquí hay dos dinámicas en juego. En primer lugar, como se explicó anteriormente, el GDPR crea algunas ventajas comparativas para las grandes empresas. En segundo lugar, las limitaciones en la recopilación y el intercambio de datos reducen el potencial para el surgimiento de un ecosistema de recopilación de datos competitivo y distribuido. Para ilustrar este punto, comparan dos escenarios:

Bajo el primero, el intercambio de datos es relativamente fácil. Esto aumenta los incentivos de las empresas para recopilar datos. Como resultado, el mercado de datos puede volverse más competitivo. Además, la mayor capacidad de las empresas para integrar diferentes conjuntos de datos reduce la necesidad de depender de una fuente de datos, ya sea interna o externa, lo que reduce el precio de los datos.

En el segundo escenario, los grandes obstáculos para compartir datos reducen la capacidad y los incentivos de algunos responsables del tratamiento para entrar u operar en el mercado. Una indicación potencial de este efecto se puede encontrar en el hecho de que algunas empresas extranjeras han salido de los mercados europeos para evitar estar sujetas al GDPR o que la cantidad de competidores pequeños y medianos en algunos mercados digitales se redujo significativamente, reduciendo así la competencia potencial. Si bien algunas empresas pueden regresar una vez que se hayan calmado las implicaciones del cumplimiento de GDPR, es posible que otras no.

La dinámica anterior, a su vez, podría fortalecer una de las principales preocupaciones planteadas en los mercados digitales: el hecho de que algunas entidades disfrutan de un poder de mercado significativo y duradero basado en gran medida en su control de grandes cantidades de datos.

Las ventajas comparativas que disfrutan estas empresas están basadas en parte en economías de escala y alcance en la recopilación y el análisis de datos, y en los efectos de red. Otras empresas, que carecen de tal variedad y volumen de fuentes de datos, pueden tener dificultades para igualar estas capacidades, especialmente cuando las ventajas de ser los primeros en actuar y los costos de cambio son altos.

Esta dificultad puede superarse si el competidor pudiera combinar los datos recopilados por numerosas fuentes. Y debido a que los datos no son rivales y, a menudo, son fácilmente replicables, los controladores de datos podrían potencialmente compartir sus datos con muchos usuarios, lo que fortalecería aún más la competencia.

Sin embargo, si las empresas encuentran grandes obstáculos para combinar los datos recopilados por fuentes externas, es posible que no puedan disfrutar de economías de escala en la misma medida que sus rivales establecidos. Esto, a su vez, podría afianzar el poder de mercado y aumentar el riesgo de monopolización (Gal y Aviv, 2020).

5. Conclusiones

El GDPR establece que la información personal solo se puede utilizar para el propósito específico en que se recopiló y con el consentimiento explícito del usuario. Esto no prohíbe el uso de datos personales para publicidad dirigida, pero su uso requiere que el usuario acepte estas condiciones.

Afortunadamente, las empresas que aspiran a prosperar en la economía digital pueden pensar de manera amplia sobre los riesgos emergentes y emprender acciones audaces desarrollando un marco de gobierno de uso de datos sólido. En lugar de depender de enfoques heredados para recopilar y almacenar datos que probablemente sean incompatibles con los riesgos emergentes, este marco debe basarse en un enfoque de privacidad por diseño, que integra la privacidad en las especificaciones arquitectónicas de las tecnologías, las prácticas comerciales y las infraestructuras físicas.

Definitivamente el GDPR representa un cambio cultural, generando nuevos procesos o modificaciones en los mismos por parte de las organizaciones, así como también nuevos riesgos. Al mismo tiempo, presenta oportunidades para ganar nuevamente la confianza de los usuarios, a partir de políticas de uso de datos responsables y que cumplan con el GDPR, y poder utilizar el nuevo escenario como un nuevo modo de diferenciarse.

Como menciona Haraminac (2021) las multas por ciberseguridad pueden ser devastadoras para las pequeñas y medianas empresas que se comportan de la misma manera que los gigantes tecnológicos. De hecho, por no desincentivar a las grandes organizaciones posiblemente aumente los riesgos de terceros de las organizaciones más pequeñas si dependen de grandes proveedores de servicios para procesar o almacenar sus datos. El seguro de ciberseguridad está disponible, pero las pólizas pueden restringir la cobertura para excluir a los actores internos y limitar la cobertura a costos específicos. Muchos problemas de ciberseguridad tienen un componente interno que puede ser difícil de identificar como externo para superar la exclusión interna.

A su vez, en el estudio sobre el impacto competitivo del GDPR que realizaron Gal y Aviv (2020), los mismos señalan que el GDPR crea algunas ventajas competitivas para las grandes empresas, y las mismas se basan en parte en economías de escala y en el alcance en la recopilación y el análisis de datos, y en los efectos de red. Otras empresas, que carecen de tal variedad y volumen de fuentes de datos, pueden tener dificultades para igualar estas capacidades, especialmente cuando las ventajas de ser los primeros en actuar y los costos de cambio son altos.

El caso AT&T demuestra cómo una de las compañías más importantes del mundo decide que sin importar que sus operaciones principales son fuera de la UE, es necesario implementar las políticas y procedimientos que establece el GDPR.

Otro caso de impacto global del GDPR que analizamos es el de las reglamentaciones locales basadas en el GDPR, como la LGPD de Brasil. El caso de SKY y cómo preparándose adecuadamente ha logrado el cumplimiento del GDPR, y por ende ya está bien encaminado para cumplir con la LGPD, por la semejanza entre las mismas.

Los cuatro entrevistados brindaron sus puntos de vista con respecto al GDPR y hubo coincidencias principalmente en cuanto al impacto global de la ley, y a que una de las principales diferencias para afrontar el GDPR por parte de las empresas que monetizan datos o de la era digital, radica en su tamaño o magnitud.

El GDPR, así como la portabilidad de datos, generaron grandes esfuerzos en los gigantes tecnológicos por adaptarse y no quedar fuera de cumplimiento. A su vez, pequeñas empresas que utilizaban modelos de monetización de datos, ya han desaparecido o lo van a hacer en el corto plazo porque no logran adaptarse ante el cambio de paradigma. El GDPR impacta ferozmente en la competitividad de estas empresas pequeñas y medianas, y a su vez generando nuevas oportunidades de negocio relacionadas con el GDPR a otras nuevas. En este caso, se podría decir que el GDPR termina funcionando como una barrera de entrada en caso de que si una empresa no cuenta con la capacidad de poder ser GDPR compliance, esta no debería operar, ya que puede enfrentar grandes problemas en un futuro cercano.

A su vez, el impacto en los gigantes tecnológicos es considerable, pero como hemos visto al contar con muchos más recursos, se les ha aminorado este impacto, a pesar de haber destinado grandes esfuerzos a capacitar a su personal e implementar las políticas y procedimientos para ser GDPR compliance. A pesar de esto, hemos visto que han recibido multas millonarias por incumplimiento.

El espectro que abarca la reglamentación es global, y trae educación y concientización en cuanto a la forma en la que los usuarios y clientes quieren que sus datos sean tratados, y estos puedan ser vistos como activos a la hora de brindarlos. Las empresas que han sabido identificar esto como una oportunidad de diferenciación y de agregarle valor al cliente mediante un claro cumplimiento del GDPR y una muestra de calidad de servicio relacionado con los datos, son los grandes ganadores. Microsoft y AT&T son 2 ejemplos satisfactorios de esto último.

6. Bibliografía

Astrid Bohé, M. H. (2013). Data Monetization in the Age of Big Data; 3; Obtenido de https://www.readkong.com/page/data-monetization-in-the-age-of-big-data-3277747

Apleyard, D. y Fieldt, A. (2003). Economía Internacional. McGraw-Hill Interamericana. Colombia.

Baltassis E., Rose J., Gourevitch A. (2018). Leveraging GDPR to Become a Trusted Data Steward. BCG Consulting. Obtenido de https://www.bcg.com/publications/2018/leveraging-gdpr-become-trusted-data-steward

Big Data: ¿En qué consiste? Su importancia, desafíos y gobernabilidad (s.f.). PowerData. Obtenido de https://www.powerdata.es/big-data

Buenadicha Sánchez, C., Galdon, G., Hermosilla, M., Loewe, D., & Pombo, C. (2019). La gestión ética de los datos. Obtenido de https://doi.org/10.18235/0001623

Business Insider (2018). How Privacy Regulation Could Impact Facebook. Obtenido de: https://www.youtube.com/watch?v=nGUy_6NRuTo

CBS News (2018). Facebook, Google roll out changes ahead of European Union's GDPR privacy rules. Obtenido de: https://www.youtube.com/watch?v=szmpt9g9LkE

CBS News (2018). Facebook rolling out privacy changes ahead of EU's data regulation. Obtenido de: https://www.youtube.com/watch?v=ql4qt40-zvw

Cook y Reichardt (1986). Métodos cualitativos y cuantitativos en investigación evaluativa. Ediciones Morata España.

Font, E. (2019). L'ús de les dades d'acord amb el Reglament General de Protecció de Dades. *Revista de biblioteconomia i documentació* (65-66). Obtenido de https://www.raco.cat/index.php/Item/article/view/353619/444617

Gal, M. S. y Aviv, O. (2020). The Competitive Effects of the GDPR. Journal of Competition Law and Economics, 16(3), 349–391. Obtenido de https://doi-org.eza.udesa.edu.ar/https://academic.oup.com/jcle/issue

Gilart I. (2017). Cómo cumplir con la nueva normativa de protección de datos mediante herramientas de GdI y backup. Obtenido de: https://www.whitebearsolutions.com/como-cumplir-con-la-nueva-normativa-de-proteccion-de-datos-mediante-herramientas-de-gdi-y-backup/?utm_source=Post%20LinkeDin&utm_medium=LinkedIn%20Pulse%20Ignacio&utm_campaign=WBS

Greengard, S. (2018). Weighing the Impact of GDPR: The EU data regulation will affect computer, Internet, and technology usage within and outside the EU; how it will play out remains to be seen. *Communications of the ACM, 61*(11), 16–18. Obtenido de https://doi-org.eza.udesa.edu.ar/10.1145/3276744

Haraminac D. (2021) GDPR and the Increasing Cost of Cybersecurity. Value Examiner. Obtenido de: https://search-ebscohost-com.eza.udesa.edu.ar/login.aspx?direct=true&db=bth&AN=152117471&lang=es&site=ehost-live

IT Governance Ltd (2019). Google's GDPR Fine | Why they received it and what it. Obtenido de: https://www.youtube.com/watch?v=72J3CQxrCFo

Ivancevich, J. y Lorenzi, P. (1997). Gestión de calidad y competitividad. 2da. Edición. McGraw-Hill. España.

Knack, G., Cohen, M., & McAllister, A. (2018). Ready for GDPR? New rules for data privacy in the European Union could have big implications for U.S. franchises. *Franchising World, 50*(8), 60–61. Obtenido de http://search.ebscohost.com.eza.udesa.edu.ar/login.aspx?direct=true&db=buh&AN=131177328&lang=es&site=ehost-live

Koch, R. (2019). What is the LGPD? Brazil's version of the GDPR. Obtenido de https://gdpr.eu/gdpr-vs-lgpd/

Kozlowski, M. (2017). Can your network deliver the potencial of the cloud? BCG Consulting. Obtenido de https://www.bcg.com/publications/2016/can-your-network-deliver-the-potential-of-the-cloud

Lăzăroiu, G., Kovacova, M., Kliestikova, J., Kubala, P., Valaskova, K., & Dengov, V. V. (2018). Data governance and automated individual decision-making in the digital privacy general data protection regulation. Administratie Si Management Public, (31), 132-142. Obtenido de http://dx.doi.org.eza.udesa.edu.ar/10.24818/amp/2018.31-09

Microsoft Cloud (2017). Microsoft's Commitment to GDPR. Obtenido de: https://www.youtube.com/watch?v=J8VdBZ88qRw

Microsoft Cloud (2017). How Microsoft supports GDPR. Obtenido de: https://www.youtube.com/watch?v=RS9kYpXxh20

Microsoft Mechanics (2018). Managing GDPR with Microsoft Services, including Data Log Exports and the Right to be Forgotten. Obtenido de: https://www.youtube.com/watch?v=oKxjwdwnWqU

Mitchell, A. (2016). GDPR: Evolutionary or revolutionary? *Journal of Direct, Data and Digital Marketing Practice, 17*(4), 217-221. Obtenido de http://dx.doi.org.eza.udesa.edu.ar/10.1057/s41263-016-0006-9

Monetización de datos: la estrategia más rentable de analytics. (2016). Logicali. Obtenido de https://blog.es.logicalis.com/analytics/monetizacion-de-datos-la-estrategia-mas-rentable-de-analytics

O'Connor, B. (2017). The final countdown to GDPR. *Accountancy Ireland, 49*(4), 52-54. Obtenido de https://search-proquest-com.eza.udesa.edu.ar/docview/1973329972?accountid=28034

Osterwalder, A., Pigneur, Y., & Tucci, C. L. (2005). Clarifying Business Models: Origins, Present, and Future of the Concept. 16. *Communications of AIS, Volume 15.* Obtenido de https://aisel.aisnet.org/cgi/viewcontent.cgi?article=3016&context=cais

Ozar B. (2021). GDPR: Why We Stopped Selling Stuff to Europe. Obtenido de: https://www.brentozar.com/archive/2017/12/gdpr-stopped-selling-stuff-europe/

Pérez Gómez, L. (2021). El Reglamento General de Protección de Datos (GDPR) de la Unión Europea y sus implicaciones en México. Nader, Hayaux Goebel. Obtenido de https://www.nhg.mx/es/el-reglamento-general-de-proteccion-de-datos-gdpr-de-la-union-europea-y-sus-implicaciones-en-mexico/

Pérez V. (2018). La GDPR mató mi negocio de venta de datos. Obtenido de: https://www.xataka.com/legislacion-y-derechos/gdpr-mato-mi-negocio-venta-datos

Porter, M. (1985). Ventaja Competitiva, creación y sostenimiento de un desempeño superior. Editorial CECSA.

Porter, M. (1990). La ventaja competitiva de las naciones. Vergara. Buenos Aires. Argentina.

Porter, M. (1997): Estrategia Competitiva. Editorial Continental, S.A. de C.V. México.

Quinn, P. (2018). Is the GDPR and its right to data portability a major enabler of citizen science? *Global Jurist, 18*(2), 81-97. Obtenido de http://dx.doi.org.eza.udesa.edu.ar/10.1515/gj-2018-0021

¿Qué es el big data? (s.f.). Oracle. Obtenido de https://www.oracle.com/ar/big-data/what-is-big-data/

Rogers, D. L. (2016). The Digital Transformation Playbook: Rethink Your Business for the Digital Age. Columbia University Press.

Sanders, A. K. (2019). The GDPR One Year Later: Protecting Privacy or Preventing Access to Information? *Tulane Law Review, 93(5), 1229–1253*. Obtenido de https://search-ebscohost-

com.eza.udesa.edu.ar/login.aspx?direct=true&db=a9h&AN=137020794&lang=es&site=ehost-live

Santamarta, S., Gandhi, R., & Bechauf, M. (2019). Big Oil, Big Data, Big Value. BCG Consulting. Obtenido de https://www.bcg.com/publications/2019/big-oil-data-value

Sutton, K. (2018). Data for Dollars. Adweek, 59(32), 10. Obtenido de http://search.ebscohost.com.eza.udesa.edu.ar/login.aspx?direct=true&db=buh&AN=133131907&lang=es&site=ehost-live

TWiT Tech Podcast Network (2019). Google gets €50M GDPR Fine. Obtenido de: https://www.youtube.com/watch?v=jvEczeRwnug

Urquhart, L., Sailaja, N., & McAuley, D. (2018). Realising the right to data portability for the domestic Internet of things. *Personal and Ubiquitous Computing*, *22*(2), 317–332. https://doi.org/10.1007/s00779-017-1069-2

Vanberg, A. D. (2018). The Right to Data Portability in the GDPR: What Lessons Can Be Learned from the EU Experience? *Journal of Internet Law, 21*(7), 1–19. Obtenido de http://search.ebscohost.com.eza.udesa.edu.ar/login.aspx?direct=true&db=buh&AN=127124747&lang=es&site=ehost-live

VESELÝ, P. (2018). Gdpr Issues from a Marketing Perspective. *Marketing Science & Inspirations, 13*(4), 43–55. Obtenido de http://search.ebscohost.com.eza.udesa.edu.ar/login.aspx?direct=true&db=buh&AN=134662922&lang=es&site=ehost-live

Washington Post Live (2018). Microsoft's Ann Johnson on impact of new GDPR privacy enforcements. Obtenido de: https://www.youtube.com/watch?v=-SDHasjRyy4

Young Koo, O. (2017). Successes and Failures of Amazon's Growth Strategies: Causes and Consequences. Institute Executive Fellow of the INSEAD Blue Ocean Strategy Institute.