UNIVERSIDAD Finis Terrae | FACULTAD DE DERECHO

EL RESGUARDO DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES, UNA COMPARACIÓN ENTRE CHILE Y ALEMANIA: ACTUALIDAD Y PERSPECTIVAS.

CHRISTEL HUBER QUEIROLO
20.020.429-8

JOSÉ PÉREZ CORNEJO
20.242.970-K

SEBASTIÁN PORTUGUEZ MORALES
20.470.306-K

Memoria presentada a la Facultad de Derecho de la Universidad Finis Terrae para optar al Título de Licenciados en Ciencias Jurídicas y Sociales

PROFESOR GUÍA: PABLO ALARCÓN JAÑA

SANTIAGO, CHILE

2023

ÍNDICE

INTRODUCCIÓN

En pleno siglo XXI se nos han presentado desafíos de diversas envergaduras dada la desenfrenada y acelerada evolución de la tecnología y del mundo cibernético, generando a su vez en nosotros un sin fin de cuestionamientos, tanto en el desarrollo de áreas de las humanidades hasta en la medicina, economía, recursos humanos, y aún más, en el derecho que nos resguarda. Esto dado a que lamentablemente en muchas ocasiones, hemos quedado atrás ante el incontenible adelanto en lo que respecta al encontrar un equilibrio entre la tecnología y el trabajo humano en destreza física o intelectual y, asimismo, en la búsqueda de respuestas o soluciones ante interrogantes que se nos presentan diariamente en la comunidad.

La informática y el mundo del internet diariamente van tomando mayor protagonismo y aunque han sido herramientas que nos han facilitado en muchos ámbitos, traen aparejadas inmensas sombras compuestas que acechan el disfrute de nuestra libertad tanto en las redes sociales como en nuestros datos personales; y aquello viene dado a que, producto de dicha navegación por el mundo del internet y al interactuar con sus diversos medios automatizados, inconscientemente hacemos entrega diaria de información sobre nuestra persona. Ejemplos de esto último parten de lo más simple como dar el nombre, domicilio, nacionalidad, gustos musicales a lo más complejo como patentes de automóviles, números de tarjetas de crédito o débito, contraseñas, sin mediar, por supuesto, si dicha conectividad entre nosotros y facilidad nos traen perjuicio y si constantemente estamos protegidos o no de ello.

A raíz de esta nueva realidad física-electrónica, es ocupación del campo normativo tener mecanismos de protección que vayan a la par con este acelerado trayecto, para encontrar una respuesta en nuestro derecho ante el blindaje de nuestra "personalidad virtual", que, a su vez, repercute en el desarrollo de nuestro ser y de lo que nos rodea. Y no es de extrañar que el derecho a la protección de datos personales cada día está tomando un cariz y un protagonismo mayor en el mundo jurídico, dada la utilidad que cada vez se le va dando a la tecnología, traduciéndose por consiguiente la ocupación principal de elaborar medidas mucho más transversales y específicos, dado que su enfoque y tipología va evolucionando y transformando en esta línea de tiempo y en el mundo.

Por lo que, es evidente brindar una especificidad, desplegar un resguardo acorde y coherente para conseguir una correcta cobertura jurídica y generar una serie de leyes o principios aplicables para dichas ramas, puesto que, a contrario sensu, si nos mantenemos dentro de un plano general similar a un "manual de instrucciones" con sentido universal, se evidencia a todas luces una falta de sentido y resguardo a toda casuística social.

Como bien se abundará, este derecho se entendió en principio como un desprendimiento de la intimidad, pero a posteriori, en algunos países se desarrolló de una manera más acabada y profunda, dando origen al derecho a la protección de datos (también conocido como derecho a la autodeterminación informativa), cuyo bien jurídico protegido es la libertad informática y su fin inmediato es garantizar a las personas un poder de control y disposición de sus datos, ya

sean estos de categoría íntimos o no, públicos o privados, con el objeto de preservar la propia identidad, dignidad y libertad de los mismos.

Por tal motivo, dentro de la comparación que efectuaremos entre dos países, que son Chile y Alemania, nos damos cuenta que en principio, el origen de este derecho precisamente emana del poco conocimiento y regulación que ambos países tienen al respecto, así como de la poca iniciativa y enfoque que le han brindado. Entonces, inmediatamente traemos a colación la siguiente interrogante: ¿qué importancia tiene la recopilación de datos, su cautela, y por qué requiere un respaldo jurídico para nosotros, sus usuarios?

Por un lado, haciendo mención de la situación de nuestro país, solamente se ha aludido en la última frase del artículo 19 Nº4 de nuestra Carta Magna que establece: …*"La Constitución asegura a todas las personas: 4º.- El respeto y protección a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley…;*[1] texto vigente que fue producto de una modificación efectuada en el año 2018 por la Ley Nº21.096, siendo antes interpretada de forma intrínseca dentro del derecho al honor y a la vida privada. Por lo que, no es de extrañar el indispensable rol que tomó nuestro ordenamiento jurídico al establecer dicho derecho de forma directa en la Constitución de la República al considerar que no fue suficiente su regulación en la Ley Nº19.628 "Sobre Protección a la Vida Privada" del año 1999.

Precisamente, todo dato recopilado nos moldea un perfil detallado sobre la persona como habitantes de una sociedad y usuarios de las redes sociales, al ser parte de nuestra vida cotidiana la mera entrega de datos de forma voluntaria. A ello se le llama el "cruce de información", que le permite a los diversos entes o plataformas del mundo cibernético tener acceso a dichos datos y trae como resultado el recabar un perfil de nuestros gustos, intereses, intimidad, etc.; siendo al final las redes sociales, claramente, un arma de doble filo, ya que si bien podemos hablar de meras plataformas que nos permiten compartir nuestras opiniones, gustos, fotografías, han sido y son utilizadas como herramientas de entablar denuncias falsas y desacreditaciones hacia personas, que a fin de cuentas no tienen un filtro de veracidad y que, finalmente, pueden llegar a afectar al destinatario en diversas formas. Esto último apunta a lo que coloquialmente conocemos por "funas", donde inclusive se pueden llegar a concretizar al efecto amenazas, constituyendo por ende una gran amonestación hacia nuestras garantías fundamentales.

Y no solo dicha premisa se refleja en Chile, sino que también en el resto del mundo, como, por ejemplo, Alemania, país de Europa Occidental, cuyo contraste en esta materia nos pareció sumamente interesante de abordar, sobre todo en lo referente a la sofisticación de su ordenamiento jurídico.

[1] (Constitución Política de la República de Chile, texto actualizado en Decreto Nº100, Segpres: fija el texto refundido, coordinado y sistematizado de la Constitución Política de la República de Chile, D.O 22-septiembre-2005)

Dentro de este tópico, el ordenamiento alemán comparte y toma el razonamiento de la Unión Europea, abordando el derecho a la protección de datos dentro del concepto y resguardo de la intimidad y sus diversas manifestaciones que puede adoptar. Sin embargo, el país de Europa Occidental, como señala Elisenda Bru Cuadrada, "*no prevé ningún precepto donde se reconozca directamente el derecho a la protección de datos, a la intimidad personal y familiar*"[2], ni tampoco elabora una observación y desarrollo acabado sobre qué consiste, cuál es su garantía, qué es lo que ocurre con los datos personales de las personas naturales y su protección, etc.; sino que efectúa una mera remisión del razonamiento compartido de la Unión Europea al considerar este derecho dentro de la personalidad, dotado de características tales como subjetivo, de defensa, de rango superior y una garantía de la libertad.

Además, hay que tener presente que, si bien el origen del derecho a la protección de datos se encuentra en Estados Unidos a inicios de los años 90 del siglo XX, el debate doctrinal en sí se encontraba precisamente en la cuna de Europa, tomando como elemento fundamental el pronunciamiento del Tribunal Constitucional Alemán en su sentencia sobre el censo de población en 1983, al establecer por primera vez este derecho denominado "*Derecho a la autodeterminación sobre información personal"*[3], pero, aun así, en lo relativo al tratamiento de datos personales y a la libre circulación de estos datos, para proteger la autodeterminación informativa de las personas naturales, aún existe un enigma que no ha sido resuelto por la Unión Europea y es que no se ha determinado "*hasta qué punto la autodeterminación informativa está dispuesta a ceder en aras del bien común y en qué medida esa tutela efectiva normativa es aplicable en la práctica, sin entorpecer de manera irremediable sustancial el tráfico cibernético y comercial al que los usuarios ya estamos acostumbrados."*[4]

Por consiguiente, podemos tener como primera visión que ambos ordenamientos presentan fortalezas y debilidades, es decir, lo que tiene un país sirve de complemento para el otro y viceversa, puesto que en una vertiente, nuestro ordenamiento contiene un análisis legal respecto al derecho de protección de datos personales, mas no presenta mayor explicación en nuestra Carta Magna ni tampoco confiere una garantía suficiente para no tener dudas acerca del beneficiario de este derecho, que son las personas (ya sean naturales o jurídicas) y su entorno en cuanto al acceso de dichos datos y quienes pueden tener dicha facultad fundamentada. Y en lo que respecta a Alemania, lo que se evidencia es que no hay dudas acerca del razonamiento que brinda la Unión Europea, y que comparte y aplica el país de Europa Occidental, y se señala en su ordenamiento una regulación para la protección de datos de las empresas, mas no para las personas naturales, y, asimismo, no se encuentra desarrollado a cabalidad el derecho de protección a los datos personales en concreto, entendiéndose que en la mayoría de los ordenamientos europeos no se pone de manifiesto la necesidad de explicar los derechos fundamentales que vinculan a los poderes legislativo, ejecutivo y judicial como derechos aplicables, puesto que nunca se ponen y deben ponerse en duda su carácter esencial para la sociedad y sus habitantes.

---

[2] (Cuadrada, 2007)

[3] (Tribunal Constitucional Federal Alemán (*Bundesverfassungsgericht*), 1983)

[4] (Castillo 2020, pág. 27)

Inclusive, hoy en día se encuentra pendiente tanto la publicación como promulgación del proyecto de ley sobre protección de datos de carácter personal, puesto que no basta con la regulación de la Ley N°19.628 del año 1999 en Chile, dado que no puede ser que la sociedad avance más rápido que las leyes, cuando lo esencial es una evolución en conjunto con todas sus particularidades, ameritando con creces el brindar la debida garantía a sus usuarios. Asimismo, para el ordenamiento alemán, no basta que se dedique un apartado en su Código Penal en su artículo 15 respecto a la violación de la esfera de la privacidad personal y confidencialidad sin autorización, aun así tiene como desafío especificar los sujetos destinatarios de la norma y desarrollar aún más el derecho en estudio.

Todo lo anteriormente sistematizado, justifica con creces una extensa investigación que aborde la problemática acerca del derecho a la protección de datos personales, su efectividad y regulación en nuestro país y en Alemania, puesto que en relación a lo expuesto se puede señalar que el diseño jurídico de la protección de datos personales en ambos países no se ha profundizado de la forma adecuada, dado que esta situación avanza desde la perspectiva social y económica de la sociedad de forma acelerada en los últimos años y que van entrelazados entre ambas aristas y deben tener el mismo tratamiento dentro de los ordenamientos jurídicos de ambos Estados.

Es por ello que en el presente trabajo desarrollamos la situación presente de este derecho en ambos países, analizamos e identificamos falencias y errores que estimamos tienen en común dichos ordenamientos respecto al resguardo de este derecho y a su regulación, culminando con una reflexión, crítica y proposición para que este derecho se encuentre completamente protegido tanto en Chile como en Alemania.

CAPÍTULO 1

INICIATIVA DE AMBOS PAÍSES RESPECTO AL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

1) Definición del derecho a la protección de datos personales

No es un factor ajeno en ninguno de nosotros sobre la importancia que es el proteger nuestros datos personales y la necesidad de brindarles resguardo en todas sus aristas posibles, puesto que aquí estamos hablando del manejo de información preciada y sensible para nosotros en muchos ámbitos.

Antes, cuando se nos venía a la mente el concepto de "datos personales", se asociaba inmediatamente con aquellos relativos a nuestra identificación, salud, familia e inclusive, datos bancarios. Pero en la actualidad, se amplía el espectro, incorporando a dicha tipología nuestros datos biométricos, de ubicación geográfica y aquellos que son recopilados diariamente por las diversas plataformas tecnológicas, que permiten conocer nuestros gustos o preferencias específicas. Y precisamente estos pueden ser comercializados sin nuestra autorización, punto que nos lleva a cuestionarnos sobre la seguridad que tienen y sobre el apuro de un blindaje mucho más concreto.

De hecho, como podemos constatar en la deducción de Thomas Cooley en su obra "Treatrice on the law of Torts", vemos lo limitado que se encuentra el campo de aplicación en esta materia y las consecuencias que no se encuentran del todo contempladas:

> El principio en que se basa dicha ley de difamación abarca un tipo de consecuencias radicalmente diferentes (...). Esta contempla solamente los perjuicios causados a la reputación, los daños causados al individuo en sus relaciones externa con la comunidad, al hacerle perder la estima de sus conciudadanos (...), para que haya lugar a la demanda por difamación lo que se hace público sobre una persona debe tener la intención directa de perjudicarle en su relación con otros, y, por tanto en lo escrito como en lo publicado, debe hacerle objeto del odio, del ridículo o del desprecio de sus conciudadanos —el efecto que puede tener lo publicado en su propia estima y en sus sentimientos no constituye un elemento esencial en el fundamento de la acción (...).[5]

El resultado de la circulación constante de datos dentro del mundo cibernético constituye en la actualidad grandes fuentes de información, de las cuales todos manejamos, pero no sabemos la verdadera intención y el objetivo para recibir dichos datos. De hecho, debido a la importancia de los mismos y a los beneficios que pueden generarle a los cibercriminales que buscan adueñarse de ellos, continuamente se está en el punto de mira el diseñar un conjunto de normas e instrucciones para proyectar una mayor seguridad.

[5] (Cooley, T. 1888, pág. 69)

En vista de lo anterior, cabe preguntarnos ¿Qué son efectivamente los datos personales? Según la Red Iberoamericana de Protección de Datos, el término dato personal se refiere a "*cualquier información de personas físicas identificadas o identificables, en forma numérica, alfabética, grafica, fotográfica, alfanumérica, acústica o de otro tipo".*

Análogamente, se puede definir como "Cualquier información vinculada o referida a una persona natural identificada o identificable. Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante información combinada con otros datos, en particular mediante un identificador, tales como el número de cédula de identidad, el análisis de elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona, excluyendo aquellos casos en que el esfuerzo de identificación sea desproporcionado*."*[6]

E incluso, la Ley Nº19.628 en nuestro país Sobre Protección de la Vida Privada, describe fácil y someramente en su artículo 2 letra f, como dato personal, "*los relativos a cualquier información concerniente a personas naturales, identificadas o identificables."*[7]

Y en concreto, dentro del mundo jurídico referente al derecho a la protección de datos personales, en las legislaciones más modernas fue reconocido y definido como un desprendimiento del derecho a la intimidad o bien, como un derecho autónomo propiamente tal, predominando en un comienzo lo primero, empezando a diseñarse y moldearse a mediados del siglo XIX al detectarse las primeras amenazas a la esfera privada y en el transcurso del tiempo, el derecho a la protección de datos personales fue cobrando un carácter mucho más autónomo a propósito de la importancia que fueron adquiriendo el mundo cibernético, las redes sociales y por supuesto, nuestros datos personales, siendo necesario por ende regular de forma independiente junto a todos los ámbitos vinculados a los datos personales, verbigracia su utilización, tratamiento, recopilación o almacenamiento. De modo que, como la informática ha empezado a evolucionar a pasos agigantados, surge una nueva relación entre datos y personas, la cual necesita ser resguardada correctamente junto a parámetros de confianza en las fuentes de información más allá de un marco original compuesto por normas referentes al derecho de la intimidad, de la imagen o del honor en sí.

Lo innovador del diseño de este derecho por ende, radica en la palpable necesidad de cambiar el eje de argumentación nacido desde la cuna de lo tradicional sobre los derechos anteriormente mencionados, reescribiendo lo que en un inicio partió desde una concepción civilista, en la cual la propiedad era el fin último del ámbito jurídico, para obtener como resultado un derecho amparado desde una corriente iusnaturalista redefinido por las nuevas condiciones de la sociedad, la tecnología y la globalización, siendo la dignidad y el libre desarrollo de la personalidad como su cimiento.

[6] (Pontificia Universidad Católica, 2023)

[7] (Ministerio Secretaría General de la Presidencia, 1999. Ley Nº19.628. *Sobre Protección de la Vida Privada.* Santiago de Chile)

A causa de lo anterior, el denominado derecho a la protección de datos o a la autodeterminación informativa "*es un derecho de tercera o cuarta generación, siendo su bien jurídico la libertad informática y persigue garantizar a cada una de las personas un poder de control y disposición sobre los datos que les afectan, sean íntimos o no, públicos o privados, con el fin de preservar la propia identidad, dignidad y libertad.*[8]

Dentro de la misma línea también se ha puntualizado como "*el derecho de toda persona física que la faculta para disponer y controlar sus datos de carácter personal, pudiendo decidir cuáles proporcionar a terceros, así como conocer quién posee esos datos y para qué, y oponerse a esa posesión o tratamiento."*[9]

Y, por último, también se ha definido por parte del Reglamento de la Unión Europea "*Medidas basadas en principios de calidad de datos, el derecho a la información en la recogida de datos, el consentimiento del afectado, los datos especialmente protegidos, los datos relativos a la salud, a la seguridad de los datos, el deber de secreto, la limitación a la comunicación y el acceso a los datos por parte de terceros (...)"*

Así pues, dicha problemática no es algo que solamente nos afecte a nivel país, sino que es una interrogante que ha sido abordada y discutida en todo el mundo, dada la globalización del uso de las tecnologías, que si bien, por un lado, nos entregan grandes facilidades, hay que ver las dos caras de la misma moneda. Y, asimismo, no solo debemos proteger nuestros datos personales respecto del tratamiento que puedan efectuar las diversas plataformas o bien de varias empresas que los manejan, sino que además se justifica dicho resguardo ante el empleo de las redes sociales, los cuales podrían llegar a hacer daño, mediante las denominadas "funas".

Esto último, dado a que, no se encuentra una institución o autoridad que fiscalice, resuelva y a fin de cuentas, prohíba la comunicación o cesión de datos personales sin el consentimiento del titular con la mera intención de concretar funas o fake news en las redes sociales, donde en muchas ocasiones no se visualiza ningún tipo de remordimiento por aquella persona que incita a la violencia de una acusación sin mayores pruebas más que su opinión respecto a un punto y su difamación en su entorno cibernético y social, como un medio de hacer justicia por vías de hecho. De esta forma, se convence al entorno social que dicho actuar goza de un espíritu cívico y que resulta beneficioso para la comunidad, convirtiendo de esta forma el internet y a la comunidad *"los nuevos inquisidores del siglo XXI y las redes"*[10]

Claramente, aquí evidenciamos un debate, pero no respecto de la veracidad o no de lo que se señalen en dichas "funas" o "fake news" o sobre su supuesta fundamentación u origen, puesto que aquello lo determina finalmente un juez, sino que aquí lo que se está en el ojo del huracán y es lo reprochable, es la masificación de dichas denuncias virtuales, cuyo único ánimo es la venganza, el juzgamiento, el humillar al receptor y a fin de cuentas, el escarnio público; con prescindencia de la presunción de inocencia del sujeto pasivo de dicha denuncia aparente, que

[8] (Labbé y Latrille. 2018, pág. 7)
[9] (Diccionario Panhispánico del Español Jurídico, 2022)
[10] (Salvador, 2019)

no nos define como Estado de Derecho, tornándose peligroso el mero hecho que el protagonista de la acusación aporte datos personales y dirección del presunto infractor de normas legales, sociales o morales, sin que una autoridad tome cartas en el asunto como el deber manda.

Por lo que, el empleo de las redes sociales y sus dos caras que habíamos mencionado como precedente, es efectivamente un arma de doble filo, puesto que puede hacer daño de una manera tan simplificada como noticia o publicación y que sea al mismo tiempo aterrador ante la falta de educación, conocimiento y cable a tierra de quienes se limitan a compartir la información sin más y que inclusive, llegan a agredir físicamente al presunto infractor del acto que no lo conocen y llegan por sí mismos a la conclusión que es el autor de los delitos, comentarios o actitudes que supuestamente ha llevado a cabo; sin contrastar mínimamente la veracidad de la información publicada y el contexto, sin medir las consecuencias que vayan a repercutir de forma inmediata o futura en la imagen pública de la persona difamada. Y pese a que, en nuestro país, por ejemplo, uno podría deducir que al presentarse dicho problema, el afectado se dirige a los Tribunales superiores de justicia por contravención del artículo 19 Nº4 de nuestra Constitución y ante la Ley Nº19.628, interponiendo recurso de protección, de todas formas aunque la medida que dictamine el juez sea eliminar la publicación o disculpas públicas, nadie se pregunta sobre el daño psicológico de la persona difamada, el cómo recuperará su imagen, qué pasa si pierde su empleo a raíz de dicha polémica y un sinfín de efectos colaterales que no tienen solución.

A modo de ejemplo, traemos a colación la sentencia de la Corte Suprema Rol N.º 2682- 2019, que señala en materia de recurso de protección, lo relacionado a la protección de datos personales y su impacto en las difamaciones que se pueden efectuar, utilizando como contexto el caso de una persona natural en sí y una clínica de asesoría veterinaria, que fueron "funadas" a través de la plataforma y red social de Facebook, mediante una publicación calificada como difamatoria. Pese a que la resolución se limitó sólo en ordenar que las publicaciones en el Facebook de la recurrida sean eliminadas de dicho perfil junto con las fotografías de la Clínica del recurrente, no es menor el hacer mención del razonamiento detrás y en su considerando octavo se menciona y se recoge lo que anteriormente hacemos mención:

> **Octavo: "**Que al haber publicado la recurrida, en su página de Facebook, información personal del recurrente Juan Moya, que se pone a disposición de terceros, sin su consentimiento, la persona reclamada ha realizado una actuación ilegal y arbitraria que contraviene la Ley N°19.628 y, en consecuencia, conculca el derecho constitucional del actor previsto en el artículo 19 numeral 4 de la Constitución Política de la República, al afectar la protección que se le debe a su vida privada y a su honra. Así se ha resuelto anteriormente por esta Corte en causa rol 95.019-2016."

En consecuencia, lo que se persigue mediante la consagración del derecho en análisis, justamente es; por un lado, la búsqueda de tutela de la propia identidad informática, esto es, la posibilidad de controlar la obtención, tenencia, tratamiento y transmisión de datos relativos a su persona, pudiendo cada uno de nosotros como usuarios y propietarios de dichos datos, decidiendo si prestarlos o no a dicha data y en qué condiciones se pueden transar. Y, por otro

lado, estamos en la averiguación de una protección hacia nuestra integridad como personas naturales ante las "funas" o "fake news".

2) Contextualización del derecho a la protección de datos personales en Chile

Cuando hacemos mención de la línea de desarrollo del derecho en relación a este tema, en América Latina, la protección de datos personales se ha desarrollado con algunas características propias. Pese a que los países mostraron un mayor crecimiento normativo en la materia y que basaron sus preceptos y leyes en el modelo europeo, todavía se está ante un terreno desconocido manifestado en el desafío de la protección de los datos, que inevitablemente se presenta con particularidades que aún no han sido resguardadas. Partiendo de la base que no existe un derecho a la protección de datos personales "latinoamericano", sino que se destaca el instituto del Habeas Data con características propias dependiendo del enfoque nacional, como bien se ha señalado en los comienzos de este derecho en Estados Unidos siendo el pionero en América al tratar esta garantía.

En la región, la protección de datos es relativamente reciente y los diversos autores justifican este retraso principalmente debido a la tardanza con que la tecnología penetró en América Latina, puesto que como hemos mencionado, la protección de datos constituye una reacción a la utilización de medios automatizados para el tratamiento de los datos personales, algo que no se percibió en dicha escala en América.

Los datos personales tienen la naturaleza jurídica de garantía constitucional, al protegerse aquellos y ser parte del derecho inherente de todas las personas a tener intimidad y vida privada, desprendido aquello del artículo 19 N°4 de nuestra Carta Magna. E inclusive, anterior a la publicación de la Ley N°21.096, la doctrina igualmente lo encaminaba y consideraba dentro de la privacidad, como un carácter o elemento del mismo.

Este razonamiento lo podemos sustentar con la deducción que realiza el profesor Pablo Contreras, quien alude a una sentencia del Tribunal Constitucional de Chile y señala lo siguiente:

> Otro antecedente nacional fue la interpretación del Tribunal Constitucional que estimó que el derecho a la protección de datos personales se encuentra recogido a partir del art. 19 N°4, que establece el derecho al respeto y protección de la vida privada . La sentencia se enmarca en un caso en que se cuestionaba la inaplicabilidad por inconstitucionalidad del precepto legal del artículo décimo, letra h) de la Ley N°20.285, sobre acceso a la información pública, que dispone la obligación de transparencia activa de la remuneración percibida en el año por cada Director, Presidente Ejecutivo o Vicepresidente Ejecutivo y Gerentes responsables de la dirección y administración superior de la empresa". Para los requirentes de inaplicabilidad, la publicidad de dicha información suponía una divulgación de información confidencial, en directa infracción del derecho a la privacidad del art. Artículo 19 Nº4 de la Constitución. En dicha oportunidad, el Tribunal Constitucional interpretó lo siguiente: "la protección de la vida privada de las personas guarda una estrecha relación con la protección de los datos

> personales, configurando lo que la doctrina llama derecho a la autodeterminación informativa. […] Ello se traduce en el control de las personas sobre sus datos y comprende el derecho a saber sobre la existencia de ficheros o archivos de registro de información de carácter personal, públicos o privados, cuáles son sus finalidades y quiénes son los responsables de los mismos, de manera que las personas concernidas puedan conocer los datos propios contenidos en dichos archivos o ficheros, teniendo el derecho a actualizarlos o a solicitar mediante el recurso de Habeas Data su rectificación o cancelación". La interpretación del Tribunal permitió anclar la autodeterminación informativa al contenido iusfundamentalmente protegido del derecho al respeto y protección de la vida privada.[11]

Siguiendo la línea de desarrollo del derecho en comento en Latinoamérica, con la entrada en vigencia de la Ley N°21.096, seguida de la protección de los datos personales regulado en el artículo 19 N.° 4 de la Constitución Política de la República, se plantea que quien sea víctima de un tratamiento inconstitucional de sus datos personales, puede interponer una acción de protección, amparada en el artículo 20 de nuestra Carta Magna. Para mayor abundamiento, es menester señalar que algunos recursos de protección respecto de datos personales que fueron fundamentados y amparados en la vulneración de la intimidad y vida privada, han sido rechazados, precisamente en atención al principio de especialidad, pues la Ley N°19.628 establece un procedimiento judicial y específico para dichas circunstancias. Aquello claramente es respecto a acciones anteriores a su protección constitucional expresa, a seis meses de su consagración constitucional, no existe claridad sobre los cambios e incidencia de aquello.

En lo que respecta a la protección de los Datos Personales a nivel legal en nuestro país, Chile, hacemos remisión de la Ley N°19.628, asimismo de la Ley N°21.096, publicada el 16 de junio del 2018. Esta última incorporó a la Constitución Política de la República, en su numeral 4º del artículo 19, sobre la protección a la vida privada y la intimidad, la protección de los datos personales, mencionando además que *el tratamiento y protección de ellos se efectuará en la forma y condiciones que determine la ley*. Con esta última frase, se remitió, entre otras leyes, a la N°19.628, la cual, como hemos ido adelantando, no es del todo eficiente para cumplir con el mandato constitucional.

El escriturar el derecho en estudio en nuestra Carta Magna fue resultado de la investigación de su historia fidedigna, acerca de sus reformas y debates que dieron fruto al reconocimiento constitucional de la protección de los datos personales como derecho trascendental, recurriendo además a fuentes doctrinales y jurisprudenciales tanto nacionales como comparadas, que permitieron finalmente ilustrarnos en dicha materia. Y pese a que su inclusión de forma autónoma a nuestro derecho y su esclarecimiento, indudablemente, fue centro de debates legislativos, se obtuvo finalmente su reconocimiento al citar especialmente dos principales sentencias constitucionales del derecho comparado sobre la materia, las cuales fueron del caso del Censo fallado por el Tribunal Constitucional Federal Alemán y la sentencia del Tribunal

[11] (Contreras, Pablo. 2020, pág. 91) (Tribunal Constitucional, Roles N° 1732-10 y 1800-10, de 21 de junio de 2011, cons. 25°)

Constitucional español sobre el alcance del derecho a la protección de datos personales en la Constitución de 1978.

Pero, no obstante a su exitosa incorporación, encontramos inmediatamente falencias en su aplicación, Sin ir más allá, la Ley Nº19.628 establece que su legislación sólo será aplicable cuando la persona (titular de los datos personales) sea una persona natural, lo cual nos parece motivo de crítica inmediata y que ahondaremos en el capítulo correspondiente, pues las personas jurídicas también poseen datos que pueden ser objetos de tratamiento y que claramente, pueden verse perjudicadas sin un correspondiente resguardo jurídico que los proteja ante eventuales manipulaciones de terceros o del mundo cibernético en sí.

Dado lo anterior es que podemos señalar que, Chile implementó un resguardo simple, general, sin mayores alcances y especificaciones, que a diferencia de Alemania que ya poseía en su Constitución el derecho a la protección de datos personales y la figura jurídica del Habeas Data, nos encontramos en una cierta desventaja dentro del campo del derecho, puesto que en nuestro sistema este resguardo se dio recién hace 23 años con la Ley Nº19.628 y es en esta misma ley en donde se establece la acción anteriormente mencionada, la cual tiene rango legal a diferencia de Alemania y los demás países europeos, que la importancia radica en que es una acción que garantiza un derecho fundamental, no siendo menester una ley específica para ello, puesto que al estar dentro del marco constitucional, no se pone en entredicho su protección y su aplicación se entiende como *"erga omnes"*.

En consecuencia, la Ley Nº19.628 quedó muy escueta, ya que a nivel internacional ya se había legislado al respecto y se tenía clara la noción de que este derecho revestía de un valor jurídico elevado, dado sus orígenes en el resguardo y protección a la vida privada como también a la intimidad, teniendo una inminente relación entre este último y la garantía a los datos personales, pero teniendo en cuenta que se trata de una figura diferente y que tiene un trato aparte como un derecho autónomo. De esta forma lo menciona el profesor Pablo Contreras, ejemplificándolo junto a una sentencia del Tribunal Constitucional Español que señala lo siguiente:

> La moción recalca principalmente el análisis del Tribunal Constitucional español. Conforme a éste, la protección de datos personales es un derecho distinto de la intimidad, tanto en su función como en su objeto y contenido. En materia de función, mientras que la intimidad protege frente invasiones al "ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad", la protección de datos personales tiene por función garantizar a su titular "un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado". Por ello, el objetivo del derecho a la protección de datos personales es más amplio que el de la intimidad. En los términos del Tribunal Constitucional español, "el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o

> no fundamentales, porque su objeto no es sólo la intimidad individual, […] sino los datos de carácter personal.[12]

En razón de lo anterior y el explicar el por qué nuestro sistema se ha quedado un poco atrás, viene dado a que no había claridad en relación a cómo tratar este "nuevo derecho" y además aún persiste la postura, de que este derecho se encuentra implícitamente en el artículo 19 N°4 de nuestra Carta Magna. Y pese a la necesidad de realizar una reforma constitucional con la Ley Nº20.096, la cual entró en vigencia en el año 2018 y que introdujo la modificación expuesta al principio de este apartado y que zanjó la discusión doctrinaria que se había suscitado con respecto a su esencia y en donde encasillar este derecho, de todas formas la Ley Nº19.628 solo resguarda el derecho desde la perspectiva comercial y económica, enfocándose netamente en la relación entre el particular y las entidades financieras públicas y privadas. Con ello, se excluye por consiguiente la situación de los datos que circulan a través de plataformas de redes sociales, servicios de "streaming", entre otros medios; los cuales se han vuelto relevante debido a la masificación de la tecnología y, por lo tanto, ya no solo podemos reducir el espectro de los datos personales a la información almacenada y guardada por entidades financieras como previamente se había planteado con la "Ley de Protección a los Datos Personales", sino que en definitiva se tiene que regular de forma más específica tanto de la perspectiva constitucional como legal.

Esto debido a que, efectuar un marco genérico como se puede ver al principio de este subcapítulo, no se obtiene como producto el fin de abarcar una mayor cantidad de situaciones que se puedan ver vulneradas en este ámbito, sino que, todo lo contrario, nos vamos quedando mucho más atrás en lo que respecta a esta línea de tiempo, ya que como hemos mencionado, inevitablemente se ha ampliado lo que se entiende por datos personales.

Hay que mencionar también que, en base a la reforma, la acción de protección se torna un elemento viable para proteger este derecho, ya que se le da un rango constitucional, siendo esto importante, debido a que como se hace mención en esta tesis, los tribunales chilenos antes del 2018 entendían que debía primar la especialidad, siendo esta la acción del Habeas Data, contenida en la Ley Nº19.628. Por lo que la acción de protección no era el camino para salvaguardar los datos personales de los particulares y a ello se debía el rechazo inmediato de los recursos constitucionales, por no ser la vía idónea hasta la entrada en vigencia de esta reforma constitucional. En consecuencia, de lo anteriormente expuesto es que en el capítulo 2 se pasarán a revisar sentencias de nuestros Tribunales Superiores de Justicia para que sea aún más claro y fundado el argumento señalado previamente.

Para cerrar este subcapítulo o punto se ha de mencionar, que Chile se ha suscrito a diversos tratados internacionales sobre el resguardo de este derecho. A modo de ejemplo podemos mencionar el Convenio N.° 108, que es el primer tratado en versar sobre datos personales. Asimismo, podemos mencionar las constantes sugerencias efectuadas por la OCDE para darle un tratamiento extensivo a esta garantía y dar como modelo a lo efectuado por el Consejo de la Unión Europea, quienes ya en 1995 estaban progresando con este tópico tan importante y

[12] (Contreras, Pablo. 2020, pág. 95)

actualmente se encuentran con una legislación más completa. Por lo pronto se puede señalar que esto no se ha llevado a cabo aún como se ha fundamentado previamente a pesar de que Chile realizó un compromiso por avanzar en esta materia.

3) Contextualización del derecho a la protección de datos personales en Alemania

Aterrizando ahora el derecho en comento dentro del marco de Europa Occidental, el derecho a la protección de datos personales en Alemania nació el 7 de octubre de 1970 a raíz de la promulgación de la Ley "Datenschutz", ley reconocida universalmente como la primera norma de protección de datos y definida como una legislación completa y acabada, que introdujo en el mundo jurídico los conceptos y términos acerca de la protección de datos, siendo tomada como un modelo para la elaboración e inspiración de normativas posteriores.

Dicha ley abarca el tratamiento de datos personales del Estado de Hesse, en la República Federal de Alemania, la cual tenía como eje la búsqueda de entregar una protección a las personas naturales ante la amenaza que representaba el tratamiento informatizado de datos nominativos por las autoridades y administraciones públicas del Estado, asimismo de los municipios y entidades locales rurales; y demás personas jurídicas de derecho público y agrupaciones sujetas a la tutela estatal. Y para garantizar el cumplimiento de sus previsiones, esta ley creó el cargo del denominado "Comisario de Protección de Datos", nombrado por el Ministro Presidente, con el objetivo de velar por la observancia de los preceptos de la propia ley y aquellos que hicieren relación al trato de los derechos personales de los ciudadanos.

En el mismo orden de ideas, uno de los principales deberes que dicha ley disponía, era la de adoptar precauciones técnicas e idóneas, incluyendo la prohibición general de terceros sobre el acceso a los datos y de mantener secreto profesional sobre los mismos. En dicho contexto, se consideran los datos personales sometidos a tratamiento por el Estado de Hesse como confidenciales. También reconoce los derechos de rectificación si los datos son inexactos y un derecho de oposición a la cesión de los datos a terceros cuando esta cesión no sea conforme a derecho, señalando a su vez, que podrán facilitarse datos para los bancos de datos y sistemas de información de la administración, para finalidades estadísticas de los organismos públicos.

Posteriormente, el 27 de enero del año 1977, se dicta la Ley Federal de Protección de Datos de la República Federal Alemana, bautizada como "Bundesdatenschutzgesetz", la cual entró en vigor el 1 de enero de 1978 y cuyo proceso legislativo y fue bastante largo, dado a que en el año 1971, el Ministro del Interior federal pidió a expertos que realizarán un informe que contuviera una completa exposición acerca de la problemática que rodeaba a la protección de datos personales, para que más adelante en el año 1973, presentará un proyecto de ley, para por fin, ser aprobada dicha ley en el año 1977. En su artículo primero, se establece que el objeto de la norma es impedir la lesión de bienes dignos de tutela de las personas interesadas, garantizando los datos relativos a su persona ante abusos cometidos con ocasión de su almacenamiento, transmisión, modificación o eliminación (elaboración de datos).

Con dicha legislación se tiene como foco el proteger no solo a personas naturales, sino que también a autoridades u otros organismos públicos, personas jurídicas, empresas u otras asociaciones de personas de derecho privado para sus propios fines, ante fines de terceros.

Asimismo, esta ley tenía como sustento la idea de un eventual abuso de la informática, considerado como posible riesgo para la intimidad, derechos y bienes de la ciudadanía. Por lo que, al igual que la ley anterior, tuvo por objeto regular todos los tratamientos de datos, tanto del sector público como del sector privado, ahondar en el principio de legitimación para el tratamiento de datos para los responsables de naturaleza pública como privada, permitiendo con ello el tratamiento de datos cuando así lo permita la propia ley u otra norma jurídica o cuando el afectado hubiera dado su consentimiento, plano que efectivamente resguarda nuestros intereses tanto como habitantes de la sociedad como usuarios de las redes sociales.

Esta norma aporta muchas novedades en términos de protección de datos, entre ellas, se encuentra la creación de un "Comisionado Federal de Protección de Datos", el cual, como se hizo mención con anterioridad, tiene por objetivo velar por el cumplimiento de la ley.

Se menciona por primera vez un deber de información al afectado tanto en el sector público, como también en el privado. También se amplía la definición de dato personal, considerando que estos son *información individual sobre las circunstancias personales o de hecho de una persona física específica o identificable*. De igual modo, se realiza una íntegra regulación acerca de los derechos de los afectados, como lo es el derecho a información sobre los datos almacenados sobre su persona, la rectificación de los datos almacenados si estos son incorrectos, el bloqueo de los datos almacenados si no se puede determinar su exactitud o inexactitud o después de que ya no se apliquen los requisitos originalmente cumplidos para el almacenamiento y por último la eliminación de los datos almacenados sobre su persona si su almacenamiento no fue admisible u opcionalmente, el derecho de bloqueo; esto después de que ya no se apliquen los requisitos originalmente cumplidos para el almacenamiento. Igualmente, se señala el derecho de publicidad, en donde se explica que las autoridades y organismos del sector públicos tienen la obligación de dar publicidad del tratamiento de datos por medio de avisos oficiales, en cambio, las entidades del sector privado, como, por ejemplo, personas, sociedades, asociaciones de personas y sucursales deben notificar el tratamiento de datos a un registro administrativo.

Avanzando con el tema, una fecha bastante importante para la evolución del derecho a la protección de datos personales en Alemania es el 15 de diciembre de 1983, donde por medio de una sentencia del Tribunal Constitucional Federal de Alemania se declara inconstitucional algunos preceptos de la Ley de Censo, la cual fue aprobada el 4 de marzo de 1982 y publicada en el Boletín de Legislación Federal con fecha de 31 de marzo de 1982. Aquello vino dado a que la Ley de Censo de población, profesiones, viviendas y centros de trabajo, obligaba a los ciudadanos a responder un cuestionario, el cual contenía preguntas sobre diferentes ámbitos de su vida personal y laboral, en donde, si un ciudadano se negaba a responder le interpondrían una sanción pecuniaria.

Es por lo anterior que el 5 de marzo de 1983, las abogadas doctora Wild y doña Sadler-Euler presentaron un recurso de amparo constitucional, el cual señalaba que la Ley de Censo lesionaba los derechos protegidos en los artículos 1, 2, 5 y 19 de la Ley Fundamental de Bonn, los cuales son, el derecho al libre desenvolvimiento de la personalidad y a la dignidad humana, la libertad de expresión y las garantías procesales.

El Tribunal Constitucional Federal de Alemania sentenció lo siguiente:

> Si no se da lugar a la resolución cautelar, pero posteriormente resultan fundados los recursos de amparo constitucional, la aplicación de la ley lesionará los derechos fundamentales de todos los ciudadanos obligados a dar información. Las repercusiones de tales lesiones de los derechos fundamentales podrían ser de importancia diversa. Serían especialmente graves si, de conformidad con el artículo 9, párrafos primero a cuarto, de la ley los datos pasarán a ser utilizados irrevocablemente dentro del marco de la gestión administrativa. Por ello, la Sala sostuvo unánimemente que la aplicación de las disposiciones en cuestión debía ser suspendida provisionalmente.[13]

Concluyendo que el fundamento del Tribunal Constitucional Federal de Alemania fue la transgresión de los artículos 1.1 y 2.1 de Ley Fundamental de Bonn, los cuales consagran la inviolabilidad de la dignidad del hombre y el derecho al libre desenvolvimiento de la personalidad, señalando también el tratamiento automatizado de datos personales puede repercutir no sólo sobre la libertad individual, sino que también sobre el interés público. En relación con lo anterior, Ernst Benda, jurista, político y juez alemán, señala lo siguiente:

> El peligro para la privacidad del individuo no radica en que se acumule información sobre él, sino más bien, en que se pierda la capacidad de disposición sobre ella y respecto a quién y con qué objeto se trasmiten. La privacidad se destruye no por la información en sí misma, sino por su transmisión disfuncional sobre la que el afectado pierde toda responsabilidad de influir.
>
> El que las informaciones puedan considerarse sensibles no dependen de que afecten circunstancias íntimas. Bajo las condiciones actuales del tratamiento automático ningún dato es insignificante. La limitación legítima del derecho a la autodeterminación informativa dependerá de a qué fin se requieren los datos, y qué posibilidades de combinación existen. A partir de ahí, deja de ser decisivo que la información requerida pertenezca a un reducto de la personalidad absolutamente protegido o a una esfera con referencias sociales.[14]

El 20 de diciembre de 1990 se emitió una actualización a la Ley Federal de Protección de Datos, derogando por consiguiente la Ley Federal de Protección de Datos de 1977, entrando en vigencia en el año 1991. Esta nueva ley trajo consigo un largo trabajo preparatorio desde la declaración de inconstitucionalidad de la Ley de Censo de Población de 1982, teniendo como

[13] (Heredero Higueras, Manuel. Sentencia del Tribunal Constitucional de la República Federal Alemana relativa a la Ley del Censo de Población de 1983).
[14] (Benda, Ernst. 2001, págs. 242 y 243)

propósito proteger a las personas físicas de los perjuicios que puedan sufrir en su derecho a la personalidad como consecuencia del manejo de sus datos personales y cuando se hace referencia al derecho a la personalidad, se refiere a la protección de los bienes y derechos inherentes a la persona por el hecho de serlo, según lo que establezca cada ordenamiento jurídico. Por tanto, la protección de datos colabora con crear las condiciones en que cada persona puede tomar por sí mismo las decisiones de su propia vida.

Inclusive, uno de los principios esenciales que contenía esta ley de 1990 es aquel que establece que la recopilación, el procesamiento y el uso de datos personales están en principio prohibidos, solo se permiten si existe una disposición legal o si el interesado ha dado su consentimiento expreso para la recopilación, el procesamiento y el uso. También se señala que todos los sistemas de procesamiento de datos deben tener como objetivo no utilizar o, mejor dicho, usar la menor cantidad de datos personales, como también, dar la posibilidad del anonimato o también de la seudonimización.

Esta ley sigue la línea de la anterior, en el sentido del control por parte del Comisionado Federal de Protección de Datos, el cual se encarga de supervisar el cumplimiento de las disposiciones de la norma jurídica en las oficinas públicas federales, controlando la recopilación, el procesamiento o su uso. Destacando que tanto los Tribunales Federales, como los organismos públicos de la Federación están obligados a apoyar al Comisionado Federal en el cumplimiento de sus funciones. También se asigna la figura del Delegado de Protección de Datos, este se encargará de garantizar la implementación de la ley en torno a los organismos no públicos que procesan datos personales de forma automática. Finalmente, un nuevo apartado de esta ley es el establecimiento de disposiciones penales y multas, en donde se señala que cualquiera que, sin autorización, reciba datos personales protegidos por la ley que no sean evidentes, guarde, cambie, transmita o quebrante una disposición de la ley, será reprimido con prisión de hasta un año o con multa. Así también se menciona que cualquier persona que intencionalmente o por negligencia actué en una infracción administrativa puede ser sancionada con una multa de hasta 50.000 marcos alemanes. (22.071.345 pesos chilenos)

Es así como hasta entonces, Alemania ha pasado por pequeñas modificaciones de su Ley Federal de Protección, siendo la última en el año 2017. Dichas metamorfosis fueron para armonizar su ámbito de protección junto con la del Reglamento General de Protección de Datos de la Unión Europea, traduciéndose sus principales modificaciones en abarcar un régimen sancionador ante conductas dentro del ámbito de la protección de datos de carácter personal que excedan del ámbito del Reglamento General de Protección de Datos, a las que se podrán imponer sanciones hasta de un máximo de 53.000 dólares. Así como también la instauración de nuevas obligaciones sobre videovigilancia en relaciones laborales, reconocimiento finalmente el derecho a ser compensado los interesados y asociaciones por el incumplimiento de obligaciones recogidas por la normativa.

CAPÍTULO 2

ESFERA DE PROTECCIÓN, ENFOQUE Y APLICACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

1) Bien jurídico protegido por el derecho a la protección de datos en ambos ordenamientos jurídicos

El marco jurídico actual de la protección a los datos personales en ambos ordenamientos ha sido resultado de la suma de varios factores, dentro de los cuales podemos hacer mención del derecho comparado, antecedentes nacionales e internacionales, doctrina, e incluso de elementos fuera del espectro jurídico tales como la extensión del derecho a la vida privada, la globalización, sentido común, entre otros.

En primer término, en lo que respecta a la aproximación de este derecho en nuestro país, podemos señalar lo siguiente. En un principio, la doctrina y la jurisprudencia mayoritaria entendían que había un bien jurídico protegido en común en el derecho a la vida privada y en el derecho a la protección de datos personales, puesto que intrínsecamente ambos perseguían el mismo objetivo, esto es, el reconocer la esfera individual de la persona en base a su personalidad y que el mismo particular puede decidir cuáles ámbitos de su vida y la de su familia quiere excluir del conocimiento de terceros, junto con evitar intromisiones no deseadas, ya sea de otros particulares, instituciones estatales u otros entes sin autorización.

Siguiendo con este razonamiento, se ha de mencionar que la redacción del derecho a la protección de datos personales presentó también otras particularidades, en relación a su objeto, fin y bien jurídico. En principio, cuando se hizo comento de la regulación de la vida privada, en un comienzo se efectuó de una forma muy concisa y acotada, estableciéndose en un tiempo después que su espectro alcanza inclusive la protección de la vida pública. Ante este último punto, se dio origen a un sinfín de debates en torno a dicha inclusión, quitándose dicho precepto textualmente del artículo y procediendo a incluir en el mismo numeral 4, los derechos a la honra y a la vida privada mucho más desarrollada. Con ello, la comisión constituyente tenía por objetivo la búsqueda de protección de la vida privada frente a la intromisión de medios de comunicación y ante el progreso exponencial de la tecnología.

No obstante, acorde a los albores de la informática y tras el análisis de antecedentes nacionales como internacionales, se comenzaba a definir por parte de nuestro país, que no se podía poner bajo el mismo umbral de protección el derecho a la protección de datos personales junto al derecho a la vida privada, puesto que, siguiendo la línea del Tribunal español, la protección de datos personales es un derecho distinto de la intimidad, tanto en términos de función como de objeto y contenido. Esto último dado a que, mientras la intimidad protege al particular frente a invasiones hacia el ámbito de la vida personal y familiar que este mismo quiere proteger de la cognición externa en contra de su voluntad, la protección de la data personal tiene por función garantizar a su titular un poder de control sobre sus datos personales, su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para su dignidad y derecho. Es decir, el fin

mediato de este último derecho no se reduce netamente al resguardo de los datos íntimos de la persona, sino que es aplicable dicha protección para cualquier tipo de dato personal; y que cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales.

Pese a reconocer el carácter independiente del derecho en comento, se opta por su inclusión textual en el mismo artículo 19 Nº4 de la Constitución Política de la República, que asegura el respeto y protección de la vida privada. Es decir, aún cuando se contempla la autonomía de la autodeterminación informativa como derecho fundamental, la reforma aplicada bajo la Ley Nº21.096 propone su regulación en dicho articulado, dado que a fin de cuentas se reconoce derivado de la intimidad y por ello, se da la razón de su ubicación. Además, se ha de mencionar que, desde un inicio en la Constitución Política de la República de 1980, la comisión constituyente tuvo consideración de tutelar la vida privada frente al peligro de los medios de comunicación, antes de la aparición y expansión del internet.

Ante dicho desglose, nos podemos cuestionar lo siguiente: ¿Cómo llegamos a esta conclusión?

Pues bien, como se hizo mención anteriormente el marco jurídico actual que conlleva el derecho a la protección de datos personales en Chile es resultado de varios elementos, dentro de los cuales es necesario remitirse a los antecedentes que fueron base de su codificación, tanto internacionales como nacionales, que a continuación procederemos a desarrollar.

Desde el enfoque del derecho comparado, la constitucionalización del derecho a la autodeterminación informativa estuvo motivada desde un principio en los diversos compromisos internacionales junto a sus estándares, que a la fecha dichos razonamientos y puntos de vista se han consolidado en nuestro país, como por ejemplo, el compromiso del Estado frente a la Organización para la Cooperación y el Desarrollo Económicos ("OCDE"), en relación a la necesidad de actualizar la regulación y protección de los datos personales en el país. Otros antecedentes fueron las referencias al Consejo de Europa y a la Unión Europea, donde en este sentido, el Convenio Nº108 para la protección de las personas con respecto a esta materia, fue invocado como parte de los fundamentos de la moción.

Y en lo que respecta a los antecedentes nacionales, se tuvieron a la vista aportes de la literatura constitucional como algunos desarrollos jurisprudenciales, aciertos apropiados para la explicación de las dos dimensiones del derecho a la protección de datos personales, que son la no interferencia de injerencias ilegítimas en el ejercicio del derecho a la privacidad; y la autodeterminación informativa, esto entendido como el derecho de las personas a controlar sus datos personales, incluso si éstos no se refieren a su intimidad. Estas dimensiones del derecho en comento fueron relevantes para determinar su carácter autónomo frente al derecho a la protección de la vida privada o intimidad.

Dentro de la misma línea, también se tuvo en consideración el concepto de "Habeas Data" en la tramitación de la reforma, aludiendo a la cátedra el profesor Humberto Nogueira, precisa para la consolidación del centro del derecho a la protección de datos personales, puesto que con ello se llegó al mismo punto que varias legislaciones compartían en ese entonces, el deber de constitucionalizar este precepto, puesto que estamos ante una facultad inherente por parte del titular de acceder, complementar o rectificar sus propios datos frente a un ente público o privado

responsable de su tratamiento. Con ello aparece el concepto de los llamados derechos "ARCO", es decir, los derechos de acceso, rectificación, cancelación y oposición, recogidas ampliamente en la doctrina nacional.

En el mismo orden de ideas, otro antecedente nacional fue la interpretación del Tribunal Constitucional, en relación a la sentencia que declaró la inaplicabilidad por inconstitucionalidad del precepto legal del artículo 10 letra h) de la Ley Nº20.285, sobre Acceso a la Información Pública, que dispuso la obligación de transparencia activa de remuneración percibida en el año por cada Director, Presidente Ejecutivo o Vicepresidente Ejecutivo y Gerentes responsables de la dirección y administración superior de la empresa, donde bajo dicho caso los requirentes estimaban que la publicidad de dicha información apunta a una divulgación de un asunto confidencial; que vulnera de forma directa el derecho a la privacidad del artículo 19 Nº4 de la Constitución Política de la República. En dicha oportunidad, el Tribunal Constitucional interpretó que "*la protección de la vida privada de las personas guarda una estrecha relación con la protección de los datos personales, configurando lo que la doctrina llama derecho a la autodeterminación informativa. […]*[15]

Es decir, resolvió que el derecho vulnerado no era el de privacidad, sino que el control de las personas sobre sus datos, en especial el tener conocimiento respecto a la existencia de archivos de registro de información de índole personal, públicos o privados, la finalidad de su tramitación y quiénes son los responsables de los mismos, de modo que el titular tenga derecho a actualizarlos o solicitar, mediante recurso de habeas data, su rectificación o cancelación. Pues bien, con la interpretación del Tribunal Constitucional, se permitió anclar la autodeterminación informativa al contenido iusfundamentalmente protegido del derecho al respeto y protección de la vida privada, puesto que como bien indica el autor Flavio Quezada *"[l]a 'estrecha relación' entre vida privada y datos personales no es más que una relación de pertenencia: la protección de los segundos se ancla constitucionalmente en la protección de la primera"*[16]. Incluso, el autor Pablo Contreras evidencia lo menester de la constitucionalización del derecho a la protección de datos personales en nuestro ordenamiento:

> Una primera respuesta puede ser de carácter pragmático: la reforma constitucional brinda un "paragua" para una futura reforma a la Ley Nº19.628 y presiona a favor de su urgencia. Esta tesis fue explícitamente defendida por uno de los creadores del proyecto, el senador Harboe, quien sostuvo que la reforma constitucional "servirá de 'paraguas' para el proyecto de ley que regula la protección y el tratamiento de datos personales y crea la Agencia de Protección de Datos Personales (boletín 11.144-07), que consagra los derechos de acceso, rectificación, cancelación, oposición y portabilidad (...) Una segunda respuesta es técnicamente más relevante: constitucionalizar el derecho a la autodeterminación informativa era necesaria para delimitar conceptual y normativamente a este frente al derecho al respeto y protección de la vida privada. Primero, porque se buscaba explicitar lo implícito en el reconocimiento que había efectuado el Tribunal Constitucional. Pero, segundo, porque al tratarse de un derecho

[15] (Sentencia del Tribunal Constitucional de Chile, Roles N° 1732-10 y 1800-10, de 21 de junio de 2011.)
[16] (Quezada, Flavio. 2012)

> "autónomo", no puede ser confundido con el contenido protegido del derecho a la privacidad.

Igualmente, se ha de recalcar, que el enfoque que toma nuestro ordenamiento jurídico es la protección de datos personales sobre los individuos en particular, esto es, a las personas naturales, dado que nuestra Carta Magna no hizo mención de la situación de las personas jurídicas y así lo ha tomado el tenor de la Ley Nº19.628. Respecto a esta última fuente, en relación a los elementos particulares del objeto del derecho a la protección de datos personales, según esta norma se puede accionar de dos vías para alcanzar su resguardo, siendo una el Habeas Data, la cual guarda similitud con el Habeas Corpus al tener ambos el fin de proteger un elemento relevante de la vida jurídica, como lo es la libertad de la autodeterminación informativa; y otra, a raíz de la reforma efectuada al artículo 19 N°4 en su último inciso, la acción de protección constitucional contemplada en el artículo 20 de la Constitución Política de la República.

Pero, reanudando el tema de inicio y que nos concierne, aún nos queda camino por recorrer en lo que respecta a la búsqueda de una protección acorde y suficiente para nuestros datos personales, para amparar nuestra seguridad y para escudar la verdad tanto en los hechos como en el derecho. Si bien existe un proyecto en curso el cual busca efectuar una completa regulación en esta temática, las dudas siguen en pie, puesto que es menester una protección y reconocimiento positivo constitucional y legal, en términos tales que exista una custodia coherente de nuestra data personal, vida privada y honor. En efecto, según las palabras de Bertelsen:

> El contenido de una base de datos puede, en efecto, representar un activo de gran valor patrimonial y de ahí la importancia de reconocer a su dueño el ejercicio exclusivo de las tradicionales facultades del dominio, esto es el uso, goce y disposición, quien podrá celebrar a su respecto los actos y contratos que permita la legislación vigente y no podrá ser privado de su propiedad sino a través del correspondiente proceso expropiatorio.[17]

Siguiendo con este análisis, por parte de Alemania, conforme al artículo 8 del Convenio Europeo de Derechos Humanos (en adelante CEDH), se ha seguido por la mayoría de la doctrina, que el derecho a la protección de datos personales se encuentra inmerso dentro de la esfera de amparo de la vida privada, familiar, del domicilio y de la correspondencia, encontrándose por ende el bien jurídico bajo la misma línea, es decir, proteger la autonomía y la dignidad humana de las personas físicas. El país de Europa Occidental, siguiendo el lineamiento de la Unión Europea, entabla y relaciona directamente ambos derechos, otorgándoles a la comunidad un ambiente de resguardo en el cual puedan desarrollar libremente su personalidad, cavilar y pensamiento crítico; conectándose por tanto con otros derechos fundamentales, tales como la libertad de expresión, de reunión y de asociación pacíficas y la libertad religiosa.

[17] (Bertelsen, Raúl. 2001)

Sin embargo, siguiendo el mismo plano que la concepción chilena, ambos derechos se diversifican en formulación y alcance, puesto que el derecho a la vida privada traduce la protección en la prohibición genérica de toda injerencia hacia la esfera personal en determinados casos, mientras que el resguardo del Habeas Data, al considerarse un derecho moderno y activo, la garantía se impregna, por un lado, en la codificación y aplicación de un sistema con mecanismos de control con el objeto de proteger los datos personales de los ciudadanos que sean elemento de tratamiento; y por otro, en el cumplimiento de componentes esenciales para concretar un coherente y seguro control de dicho procesamiento de datos.

Producto de lo anterior, la Unión Europea (en adelante UE) también ha reconocido la protección de datos como un derecho fundamental específico, recogido este último en el artículo 16 del Tratado de Funcionamiento de la UE, donde, como bien hicimos mención en puntos anteriores, la protección se reguló por primera vez en la Directiva sobre esta temática del Habeas Data en el año 1995, pero en vista de los rápidos avances tecnológicos, se adoptó en 2016 una nueva legislación para ajustar la normativa a dicha era del mundo cibernético del cual somos todos protagonistas, testigos y expectantes.

No obstante, es menester hacer mención de, que el enfoque del derecho a la protección de datos personales en la UE se encuentra orientado a una política policial, es decir, para el cumplimiento de fines de prevención, investigación, detección y enjuiciamiento de infracciones penales o a la ejecución misma de las sanciones que se deduzcan, producto de la contravención hacia dicho derecho fundamental, según así lo ha hecho presente la Directiva de la UE desde 2017 a la fecha. Esto producto de lo señalado en el mismo artículo 8 de la CEDH de la UE, puesto que no solo reconoce el derecho a la protección de los datos personales, sino que además señala explícitamente los valores fundamentales asociados a esta misma garantía; aludiendo que el tratamiento de la data personal de cada uno de nosotros como usuarios y propietarios ha de ser leal y destinado netamente a fines concretos, contando asimismo con nuestro debido consentimiento, rigiéndose por ende en el fundamento de este derecho legítimo. Y tal como lo hemos hecho presente, aquello gravita y se desenvuelve en una simple lógica, los ciudadanos deben tener derecho de acceso y rectificación de sus datos personales y en caso de usarse, dicho tratamiento debe ser controlado por una autoridad independiente, ya no estamos ante una simple definición sobre lo que son los datos personales, sino que la gama se ha ampliado en términos tales que se ha tornado mucho más compleja su aplicación y discernimiento en comparación con el derecho a la vida privada. Al efecto, tomamos las palabras del autor Helmut Satzger respecto a la cibercriminalidad:

> Por supuesto, en una sociedad de la información –como la moderna– no puede haber "espacios libres de derecho" y ello aplica, sobre todo, para la creación de las normas penales que realizan la clásica labor de proteger los bienes jurídicos, las cuales deben adaptarse a las nuevas circunstancias y ser, al mismo tiempo, exigibles en la práctica. Internet no está limitada a las fronteras nacionales; por eso, un Estado no puede enfrentar en solitario estas nuevas formas de delincuencia; de ahí la necesidad de

> iniciativa internacionales como las diseñadas en los últimos años que permitan influir significativamente en los sistemas judiciales nacionales.[18]

En efecto, el instrumento internacional primordial dentro de esta logística y política policial, ha sido actualmente el Convenio de Budapest, tratado multilateral de derecho público suscrito el 23 de noviembre de 2001 "contra la cibercriminalidad", adherido no solo por países miembros del Consejo de Europa, sino que, también ratificado por otros Estados, tales como Estados Unidos, Canadá, Sudáfrica, Australia y Japón.

Con más detalle, el objetivo del Convenio de Budapest es, por un lado, reflejar lo importante que es el combatir la cibercriminalidad a nivel internacional y por otra arista, establece una política criminal propia para enfrentar los desafíos que trae aparejado dicha amenaza, brindándole a su vez a las personas una armonización ideal de la legislación en cada uno de los países miembros, un perfeccionamiento de la cooperación internacional y por último, crear medidas procesales penales conjuntas.

Ahora bien, las infracciones de los cuales hace referencia el Convenio, apuntan en primer lugar el acceso ilícito de todo o parte del sistema informático y su intercepción en los datos, atendiendo al término conocido coloquialmente como "*hacking"* o inclusive, dentro de la misma línea encontramos el delito de abuso de los equipos e instrumentos técnicos para alcanzar la misma finalidad, que es el producir, vender y obtener herramientas de acceso o de *hacking*. Asimismo, hace referencia a los diversos atentados contra la integridad de dicha data personal global y del mismo sistema que trata dichos datos personales, como bien señala a modo ejemplar el caso de la implantación o transmisión de virus informáticos con la finalidad de afectar todo un sistema computacional, pudiendo la persona controlarlo desde un ordenador externo. Y de igual forma, se puede hacer mención de variados ataques en las navegaciones de servicios o plataformas, negándole el acceso a los usuarios. Y a ello se suman las complejidades de la globalidad, ubicuidad de los datos informáticos y la velocidad con que viajan los sistemas de información, donde en principio se genera un gran laberinto y verdaderos retos.

Inclusive, ante este nuevo desafío que nos presenta el mundo cibernético, inevitable cabe plantearse, si el brindar la protección penal requerida y a la confidencialidad, integralidad y disponibilidad de los sistemas informáticos y redes de la data, constituiría o no un nuevo bien jurídico independiente.

En base a dicho planteamiento, especialmente respecto a la autodeterminación informática que traduce el deseo del particular de mantener reservado aspectos de su vida personal y de los cuales estima que se ven amenazados por el uso de la tecnología, al efecto la doctrina y la jurisprudencia se han pronunciado y han permitido el reconocimiento de un nuevo bien jurídico en el derecho penal. Sin embargo, si bien se ha hecho mención en reiteradas sentencias sobre este nuevo derecho fundamental de carácter informático implícito en la garantía de los datos personales, surge una inmediata crítica, la cual es la carencia de justificación explícita

[18] (Satzger, Helmut, pág. 12)

constitucional, siendo esta garantía de la confidencialidad e integridad de los sistemas de tecnología de información una mera expresión implícita dentro de los derechos fundamentales regulados en la Ley Fundamental general como el derecho al libre desarrollo de la personalidad que también fue base para reconocer la autodeterminación informática por parte del Tribunal Constitucional. Como bien puso en énfasis la autora María Lazpita Gurtubay en su análisis:

> La implantación discontinua, pero generalizada, de las Nuevas Tecnologías de la Información ha supuesto una amenaza para los Derechos Funda- mentales del hombre y ha desembocado en la articulación de leyes tutelares de los sujetos de datos, con la intención de lograr un control mínimo pero eficaz que no bloqueara el desarrollo tecnológico y económico. Desde una perspectiva estrictamente europea, todas las leyes de protección de datos tienen en común las siguientes condiciones: el reconocimiento del carácter excepcional*(Unique Nature)* del procesamiento de datos personales; la inequívoca manifestación de los propósitos de los requerimientos para procesar informaciones personales; la continua revisión actualizadora de las normas y la previsión de una autoridad independiente de control[19]

Es decir, esencialmente nos demuestra una vez el razonamiento para que en el derecho penal se inculque el alcance de la informática junto al bien jurídico trascendental compuesto por datos e informaciones intangibles, dado que esta rama jurídica no puede quedarse dentro del plano tradicional frente a este tipo de cambios y mutaciones, más bien debe ser dinámico y preventivo para evitar los diversos atentados contra los derechos fundamentales de las personas y de la sociedad plena.

2) Acceso y control de datos personales según lo fallado por los tribunales superiores de justicia de nuestro país

De acuerdo a los ideales que hemos expuesto, en base a la importancia, protagonismo, masificación y evolución de las redes sociales, a continuación, pasamos a revisar tres sentencias falladas por la Corte Suprema y por Cortes de Apelaciones de Chile, en torno a la protección de datos personales en el internet y más concretamente en las redes sociales.

En primer término, en la Causa Rol 450-2018, dictada por la Sala Tercera Constitucional de la Corte Suprema, con fecha 22 de mayo del 2018, don Cristián Muñoz Roa interpone recurso de protección en contra de doña Victoria Lizama Rivas, indicando que el día 17 de octubre del año 2017 le llegaron mensajes de Whatsapp, los cuales comunicaban que había una publicación en Facebook, cuyo contenido y fotografías eran difamatorios hacia su persona. Esto producto de que doña Victoria Lizama, su ex pareja, realizara una publicación en su perfil personal de Facebook (el cual se encontraba visible y público), etiquetando a dos ex parejas de don Cristián Muñoz, que lo señalaban que era un acosador, maltratador de mujeres, misógino y mentiroso, entregando sus correspondientes vivencias personales con don Cristián.

[19] (Lazpita Gurtubay, M, pág. 415)

Este último señala que dichas tres denuncias son falsas y que no existe ninguna denuncia por violencia intrafamiliar en su contra, señalando que dicha publicación afecta su honra por ser difamatoria. Siendo entonces vulnerado en las garantías constitucionales establecidas en el artículo 19 N°1, 4 y 24 de la Constitución Política de la República, solicitando la eliminación de la publicación de Facebook.

Por otra parte, doña Victoria Lizama contesta el recurso de protección, señalando que la publicación mencionada nunca tuvo por intención injuriar ni dañar la imagen de Cristián Muñoz, sino que utilizó dicho medio como forma de entablar una denuncia pública en el marco de la campaña internacional "#METOO", la cual fue una campaña realizada por una actriz estadounidense, para evidenciar y visibilizar el acoso sexual y la violencia de género. A raíz de ello, las tres mujeres decidieron aprovechar dicha campaña para hacer públicas sus experiencias y, con ello, poder contribuir a evitar que don Cristián continúe agrediendo a otras mujeres. Agregando que durante varios meses sufrió de constantes acosos virtuales por parte de don Cristián, destacando su alto contenido sexual y controlador, pidiendo en varias oportunidades su alejamiento con ciertas personas en particular, esto apoyado en informes psicológicos de los terapeutas que apoyaron su proceso de terapia reparatoria por lo vivido.

La Corte de Apelaciones, al efecto, señala lo siguiente en su considerando octavo:

> "Que, en principio, la creación de un perfil en la red internet, y específicamente en la página Facebook, normalmente no ha de estimarse una acción arbitraria o ilegal. Sin embargo, los términos contenidos en la misma, así como las apreciaciones que se refieran en una página o perfil público, sí son factibles de ser considerados, desde una perspectiva jurídica. En relación a lo previamente consignado, analizados los fundamentos de la acción intentada, es dable apreciar que se trata de hechos que si bien efectivamente presentan características particulares que implican a priori un agravio, ofensa o menoscabo, aparentemente aptos para afectar los derechos del recurrente, lo cierto es que, como lo expresó la propia parte recurrente, se trata en esencia de adjetivos o calificaciones que tienen una connotación jurisdiccional precisa y específica, esto es, susceptibles de ser investigados y eventualmente sancionados en sede penal, ámbito del derecho precisamente establecido para la tramitación de asuntos como los que el recurrente plantea.
>
> En estas circunstancias, resulta necesario concluir que el recurrente dispone de otros derechos precisos y específicos para accionar, y se encuentra perfectamente facultado para instar o iniciar el respectivo procedimiento investigativo, el cual, a su vez, constituye el camino más idóneo y de lato conocimiento, para establecer o descartar la existencia de vulneraciones de derechos, o de situaciones que afecten bienes jurídicos de su parte como los que se aprecian en el sustrato fáctico de su libelo, en términos tales de constituir eventuales ilícitos particulares, como lo expresó la misma parte recurrente al momento de presentar su recurso en que, precisamente los calificó como posibles imputaciones injuriosas."

Por lo tanto, rechaza el recurso deducido argumentando que existe un diverso procedimiento judicial, el cual es más adecuado y directo para discutir esta materia en relación a los temas de fondo de que se trata. A través de la vía investigativa y/o jurisdiccional, será posible establecer el mérito de las conductas cuestionadas y su clasificación jurídica, si existiera mérito para ello. Destacando que la Ministra suplente María Cecilia González Diez, votó en contra, estando por acoger el recurso de protección en virtud de los siguientes fundamentos:

> "1.- Que, actualmente, y más allá de que la vía penal es idónea para recurrir por aquellos dichos que además de afectar la honra de la persona, sean constitutivos de delito a través de las figuras de injuria y/o calumnia, la acción de protección constitucional es la vía por la cual se está conociendo y adoptando las medidas inmediatas de restablecimiento del derecho del recurrente que se ha visto afectado por una publicación en Facebook.
>
> 2.- Que, cabe destacar que, como base de la discusión, y sin importar la sede en la cual se decida ventilar el asunto, ni el medio de comunicación o plataforma social en el cual se haga, el derecho a la honra debe ser debidamente ponderado con la libertad de expresión, en especial, cuando las posibles expresiones injuriosas y/o calumniosas han sido emitidas a través de un medio de comunicación social."

En tanto, la Corte Suprema señala que dicho conflicto versa acerca de la contraposición entre el derecho a la honra y la libertad de expresión. Destacando el considerando undécimo que menciona lo siguiente:

> "Undécimo: Que, en este orden de ideas, conviene tener presente que el artículo 1, inciso 2° de la Ley N°19.628 sobre Protección de la vida privada y tratamiento de datos de carácter personal establece el derecho a tratar los datos personales de manera concordante con ésta. Asimismo, ha expresado en el inciso 1° del mismo artículo que la regulación del tratamiento de datos personales que por ella se hace no será aplicable a los casos de ejercicio de las libertades de emitir opinión e informar.
>
> Pero también ha proporcionado, en su artículo 2, letra f), un concepto de datos de carácter personal o datos personales diciendo que son los relativos a cualquier información concerniente a personas naturales, identificadas o identificables, diferenciándolos expresamente de los que denominó datos sensibles, definidos en el literal g) como aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual, disponiendo en su artículo 10 que no pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares."

Destacando que los datos en la plataforma de Facebook se publican sin aplicar las herramientas que permiten restringir el acceso, esto quiere decir que pueden ser utilizados en algún proceso de tratamiento de datos, en tanto no se trate de los datos sensibles señalados anteriormente. De esta manera, la recurrida utilizó datos sensibles del recurrente sin que la hubiera autorizado para realizarlo y que, en base a los antecedentes, no existe algún elemento que concluya que las atribuciones de mala conducta que doña Victoria formuló a don Cristián en la publicación de Facebook resultan plausibles. Por lo tanto, la Corte Suprema concluyó que la publicación que realizó la recurrida tiene un carácter abusivo y que ha resultado lesiva para los derechos a la honra, a la intimidad y la privacidad del recurrente, el cual ha sido sometido al escarnio público, sufriendo amenazas y descalificaciones, constituyendo una pena infamante aplicada por quien no es un órgano jurisdiccional. Por lo tanto, revoca la sentencia apelada y declara que se acoge el recurso de protección interpuesto por don Cristián Muñoz Roa en contra de doña Victoria Eugenia Lizama Rivas, ordenando eliminar la publicación de Facebook y abstenerse de realizar cualquier otra comunicación pública de similares características.

En segundo lugar, tenemos otro caso bajo esta misma materia sobre el internet y las coloquialmente afamadas "funas", la causa Rol 58.531-2020, dictada por la Sala Tercera Constitucional de la Corte Suprema de Chile, el día 7 de agosto de 2020.

En esta ocasión, don Nicolás Mendoza Candía deduce recurso de protección en contra de doña Carolina Ramírez Fernández, quien el 1 de diciembre de 2019 publicó en la red social Instagram una historia autobiográfica, donde se visualiza una fotografía del recurrente con el siguiente texto: "funa Nicolás Mendoza Candía", junto con el relato de hechos que habrían ocurrido en el mes de mayo de 2017, en donde se le imputa una conducta de abuso sexual en su contra. Dicha publicación se masificó en las redes sociales, generando un descrédito a su honra dentro de su entorno social, familiar, vecinal y universitario, siendo por consiguiente víctima de amenazas por las mismas plataformas virtuales. Siendo entonces que la conducta de la recurrida vulnera las garantías constitucionales de los números 2 y 4 del artículo 19 de la Constitución Política de la República, argumentado en que, la única forma legal de imputar, denunciar, formalizar o declarar una responsabilidad penal respecto de una persona, es a través de una sentencia condenatoria ejecutoriada, que ha de provenir de un debido proceso por un órgano público competente y no mediante afirmaciones unilaterales por vía de una red social.

Por su parte, doña Carolina Ramírez Fernández contesta el recurso señalando que dicha historia publicada en su red social, es lo que le ocurrió, quién no aguanto más el temor y la vergüenza, publicando dicha "funa" en contra de don Nicolás. Señala que los hechos sucedieron el 19 de mayo de 2017, cuando ella tenía 16 años, y se encontraba al cuidado del recurrente, él había aceptado ejercer el cuidado responsable junto a otros deportistas mayores de edad, que son miembros del equipo deportivo al cual pertenecía. Menciona que por miedo y vergüenza no realizó la denuncia penal en contra de su agresor ni comentó los hechos con su familia, amigos y equipo deportivo. Pero finalmente se retiró del club, para así no tener relación con don Nicolás.

Doña Carolina, al evidenciar a otra mujer realizando una denuncia social en contra de un hombre por una situación parecida a la suya, decidió compartir en su red social una historia en la que denunció los hechos de los que había sido víctima, publicando con ella una fotografía de don Nicolás. Destacando que se encuentra en una terapia psicológica reparatoria para sobrellevar el proceso de revictimización. Finalizando con que considera que la acción de protección no es el procedimiento idóneo para verificar la veracidad de los hechos que fundan la publicación. La Corte de Apelaciones, en este caso, señala en su considerando tercero:

> "Que los antecedentes referidos por el recurrente dan cuenta de hechos pueden ser constitutivos de un ilícito –injurias o calumnias- y por su parte, también lo son los actos referidos por la recurrida, quien además exige la oportunidad de acreditar su veracidad. De esta manera y dada la naturaleza cautelar del recurso de protección, aparece que éste no resulta idóneo para resolver la materia propuesta, pero sí lo sería el procedimiento penal correspondiente, con amplias posibilidades de prueba y discusión."

Por lo tanto, la Corte de Apelaciones de Concepción estima que en el caso que el recurrente considere ser víctima del delito de injurias o calumnias, debe proceder por la vía procesal correspondiente. Argumentando que los derechos fundamentales no son absolutos, puesto que admiten limitaciones frente al ejercicio de otros derechos fundamentales, donde el ordenamiento jurídico chileno consagra un amplio espectro de libertad de expresión e información, optando por proteger la honra y vida privada de las personas, donde el Tribunal Constitucional ha sostenido que, bajo ciertas circunstancias, la libertad de expresión puede constituirse como causal de justificación de imputaciones que puedan afectar el honor y la honra (Rol 1463).

Es por lo anterior que la Corte de Apelaciones de Concepción rechazó, sin costas, el recurso de protección deducido por don Nicolás Mendoza Candía. Destacando que la Ministra Carola Rivas Vargas concurre al rechazo del recurso señalando algunas consideraciones:

> "1.- Que, resulta importante consignar para la decisión de este recurso que, tal como expresa la recurrida en su informe, la publicación en cuestión constituye un acto de autoayuda o de reparación personal, íntimamente relacionado con la develación de un presunto delito sexual.
>
> 2.- Que, lo anterior, resuelta del todo relevante puesto que si bien, no es posible justificar la autotutela, es preciso evidenciar que las actuaciones de una víctima de un delito sexual no se sostienen en la sola exigencia de una denuncia o una querella, puesto que el escenario donde han de enfrentar su experiencia traumática, es distinto al exigido para otro tipos de delitos, precisamente porque la afectación es a su indemnidad, intimidad, libertad sexual, por tanto es necesario visibilizar a dicha víctima en este específico escenario, donde la forma de enfrentar su vivencia, es también particular."

Finalmente, la Corte Suprema señala que si bien, el artículo 20 de la Carta Fundamental no enumera determinadamente entre las garantías susceptibles de ampararse por ese arbitrio cautelar al derecho a la propia imagen, la doctrina y jurisprudencia coinciden en que su protección deviene y encuadra en el artículo 19 Nº4 de la Constitución Política de la República, por encontrarse implícitamente comprendida en el atributo de privacidad de la persona[20]. Así lo señala en su considerando octavo:

> "Que, por lo mismo, se ha señalado que: La primera y más antigua dimensión de la protección a la propia imagen se vincula estrechamente con el derecho a la vida privada, hecho que estuvo presente en los redactores del artículo que dio comienzo a la moderna discusión del right to privacy.
>
> El titular del derecho a la privacidad de su propia imagen tiene la facultad de controlarla y, por tanto, el poder de impedir la divulgación, publicación o exhibición de los rasgos que la singularizan y comprende, naturalmente, su imagen propiamente tal, su voz, y su nombre, protegiendo con esto el ámbito privado de su persona y su entorno familiar, el cual queda, indudablemente, sustraído al conocimiento del alcance de terceros. Esta protección reviste especial importancia en la actualidad, dado el creciente desarrollo de tecnologías y procedimientos que posibilitan enormemente la captación, difusión y deformación de imágenes de las personas.
>
> No obstante que la Constitución de 1980 no incorporó el derecho a la propia imagen, como un derecho fundamental, los tribunales superiores de justicia de nuestro país han acogido acciones vinculadas a las dimensiones que reviste su protección. De este modo, la jurisprudencia nacional se ha pronunciado, precisamente, respecto del derecho a la propia imagen, vinculándolo con el derecho a la vida privada, al honor y a su crédito comercial. (Anguita Ramírez, Pedro. La Protección de Datos Personales y el Derecho a la Vida Privada. Régimen Jurídico. Jurisprudencia y Derecho Comparado, Editorial Jurídica de Chile, año 2007, pp. 155 -156)."

Asimismo, menciona que se produce una colisión entre las garantías constitucionales del derecho a la honra y el de la libertad de expresión, las cuales deben ser debidamente ponderadas. En donde, dentro del derecho a la honra, se encuentra consagrado también el derecho al buen nombre, el cual se refiere al concepto que del individuo tienen los demás miembros de la sociedad en relación con su comportamiento, honestidad, decoro, condiciones humanas y profesionales, derecho que se vio afectado en tanto se publica en una red social afirmaciones deshonrosas a su respecto, que distorsionan el concepto público que se tiene del individuo y que tienden a socavar el prestigio y la confianza del individuo con su entorno. Destacando que la libertad de expresión no tiene un carácter de absoluto y queda limitada por el derecho al buen nombre.

[20] (Sentencia Corte Suprema de Santiago, Sala Primera, Rol 9970-2015, 28 de Septiembre de 2015)

Es por lo anterior que la Corte Suprema concluye que las expresiones realizadas por la recurrida, por medio de la red social, generaron una perturbación del derecho a la propia imagen del recurrente y su derecho a la honra consagrado en el número 4 del artículo 19 de la Constitución Política de la República. Por lo tanto, se revoca la sentencia apelada y se acoge el recurso de protección deducido por don Nicolás Mendoza Candía, disponiendo que la recurrida deberá eliminar de inmediato la publicación realizada en la red social Instagram.

En otro orden de ideas, una materia que se tiene que tener en consideración en torno a la protección de datos personales, como se señaló anteriormente, es la materia financiera y comercial. Y en este sentido podemos examinar el tercer caso sujeto a análisis dentro de este ítem, la causa Rol 32.337-2020, con sentencia dictada por la Sala Tercera Constitucional de la Corte Suprema, el día 29 de abril de 2020.

Bajo este acontecimiento, doña Sol Madrid Iturriaga deduce recurso de protección en contra de Banco Scotiabank Chile S.A. Doña Sol manifiesta que con fecha 27 de mayo de 2008, suscribió el Contrato de Apertura de Línea de Crédito para Estudiantes de Educación Superior con Garantía Estatal, también llamado Crédito con Aval del Estado (CAE), con el Banco del Desarrollo y cuyo sucesor legal es la parte recurrida. Señala que al no pagar tres cuotas consecutivas se aceleró el crédito en una sola cuota como plazo vencido, por lo que, según el mandato conferido, en la cláusula N°15 y N°16, se suscribieron tres pagarés a plazo con fecha 21 de noviembre de 2016. Es por lo anterior que dicho banco ingresó demanda ejecutiva con fecha 29 de noviembre de 2016, en la causa Rol C-29398-2016 D del 21º Juzgado Civil de Santiago, dictando sentencia definitiva que declaró prescrito los pagarés antes individualizados con fecha de 21 de diciembre de 2018, destacando que dicha sentencia se encuentra firme y ejecutoriada.

Agrega que la obligación que tiene el acreedor de eliminar esos registros en virtud del artículo 19 de la Ley N°19.628 es de 7 días, la que comienza a correr desde que la sentencia se encuentra firme y ejecutoriada, por lo que Banco Scotiabank Chile S.A. excedió dicho plazo estando en total conocimiento de la mencionada sentencia e informó las letras separadamente a la Cámara de Comercio. Vulnerando así el artículo 19 Nº4 de la Constitución Política de la República, de modo que dicho banco ha ejercido atribuciones en forma indebida y contrariando el artículo 6 de la Ley N°19.628 sobre Protección de la Vida Privada, que señala que los datos personales deben ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado. Es por lo anterior que pide eliminar la deuda antes dicha de los registros de morosos de la Cámara de Comercio; Sistema Nacional de Comunicaciones Financieras S.A.; Equifax Chile S.A.; Sistemas Integrados de Información S.A. y en la Comisión para el Mercado Financiero.

La parte recurrida explica que, con fecha 8 de noviembre de 2019, Equifax Chile S.A. envió un informe, señalando que la recurrente posee en la actualidad morosidades publicadas en sus registros, y que las morosidades aportadas por el recurrido Scotiabank Sud Americano pertenecen a la base de datos “BOLCOM”, cuyo responsable es la Cámara de Comercio de Santiago.

Asimismo, el 12 de noviembre de 2019 evacuó oficio la Cámara de Comercio de Santiago, quien señaló que la recurrente en ningún momento les ha solicitado la eliminación de los datos que en este banco de datos se publican. No obstante, lo anterior, expresa que habiendo tomado conocimiento de la declaración de prescripción que la recurrente invoca con motivo de la interposición del recurso, y habiéndose acreditado que la respectiva sentencia se encuentra ejecutoriada, se ha dispuesto la eliminación de las anotaciones que doña Sol registraba en el Boletín de Informaciones Comerciales. Además, en la fecha anteriormente señalada, el recurrido solicitó el rechazo del recurso, con costas, argumentando que se ha desinformado la deuda ante la Comisión para el Mercado Financiero y se ha procedido a realizar trámites administrativos tendientes a borrar de la citada entidad la deuda de la recurrente. Sin embargo, respecto de la información que se mantiene en DICOM, la misma recurrente puede realizar la actuación necesaria y solicitar el borrado de su deuda ante DICOM. Añadiendo que no procede la acción cautelar cuando hay un régimen especial de reclamos, como el que se encuentra regulado en la Ley N°19.628, sobre Protección de Datos de Carácter Personal.

Agregando que la recurrente confunde dos registros distintos: el Registro que lleva la Superintendencia de Bancos e Instituciones Financieras de conformidad al artículo 14 de la Ley de Bancos en relación al Capítulo 18-5 de la RAN y el Boletín Comercial. Por lo tanto, no tiene relación alguna la normativa citada con el Boletín Oficial, de este modo, afirma que no existe la infracción legal imputada por la recurrente. Finalmente, destacando que no existe acto ilegal o arbitrario, ya que sólo se envió a la Cámara de Comercio la información que por expresa disposición de la ley se encuentra obligado a entregar, por lo que cualquier error en la publicación no es atribuible a Scotiabank Chile. La Corte de Apelaciones de Santiago explica lo siguiente en su considerando tercero:

> "Que, evacuado informe por la Cámara Comercio de Santiago A.G., indicó que con ocasión de la presente acción se ha dispuesto la eliminación de las anotaciones que la actora registraba en el Boletín de Informaciones Comerciales, de lo cual da cuenta el certificado que se acompañó. Dicha información fue refrendada también por Servicios Integrados de Información S.A, la Comisión para el Mercado Financiero y el propio recurrido."

Es por lo anterior que la Corte de Apelaciones considera que el acto objeto de reproche ya no existe, pues la medida reparatoria que se perseguía mediante la interposición de la presente acción ya está cumplida, de modo que el recurso de protección ha perdido oportunidad. En consecuencia, rechaza el recurso de protección. Al efecto, es importante destacar que el Ministro Sr. Caro, votó en contra, quien estuvo por acoger, con costas, la presente acción, señalando lo siguiente:

> "Toda vez que atendido a lo expuesto por el propio recurrido, éste habría desinformado la deuda sub lite recién con ocasión de la interposición del recurso de protección de marras, acreditándose por tanto que éste incumplió su obligación de desinformar la deuda en virtud del artículo 19 de la Ley N°19.628, cuestión que debería haber realizado en consideración a la declaración de prescripción de la misma por el 21° Juzgado Civil de Santiago con fecha 21 de diciembre del 2018, siendo esta acción constitucional

> plenamente apta para resguardar los derechos que se reclaman como afectados, por cuanto para ser acogida no se requiere una discusión de lato conocimiento, dado que se está frente a un derecho indubitado de la actora que emana de la declaración judicial de prescripción de la deuda. La existencia de una normativa especial que reconozca el ejercicio de acciones de orden jurisdiccional, no es óbice para intentar este recurso de orden constitucional, por cuanto el constituyente en el artículo 20 dispone que es "sin perjuicio de los demás derechos que pueda hacer valer ante la autoridad o los tribunales correspondientes", por lo que corresponde desestimar las alegaciones de la recurrida en este sentido."

Por el contrario, la Corte Suprema señaló que se advierte que la Comisión para el Mercado Financiero, en sus Estados Deudores N°5186983 y N°5203441, informó que doña Sol registra una deuda con el recurrido, lo cual da cuenta que éste no desinformo la referida acreencia incumpliendo lo dispuesto en el artículo 6 de la Ley N°19.628, que dispone lo siguiente:

> "Los datos personales deberán ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado. Han de ser modificados cuando sean erróneos, inexactos, equívocos o incompletos. Se bloquearán los datos personales cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa y respecto de los cuales no corresponda la cancelación. El responsable del banco de datos personales procederá a la eliminación, modificación o bloqueo de los datos, en su caso, sin necesidad de requerimiento del titular".

Y que, asimismo, se quebrantó lo expuesto en el inciso segundo del artículo 19 de la Ley Nº19.628, el cual expresa lo siguiente:

> "Al efectuarse el pago o extinguirse la obligación por otro modo en que intervenga directamente el acreedor, éste avisará tal hecho, a más tardar dentro de los siguientes siete días hábiles, al responsable del registro o banco de datos accesible al público que en su oportunidad comunicó el protesto o la morosidad, a fin de que consigne el nuevo dato que corresponda, previo pago de la tarifa si fuere procedente, con cargo al deudor."

Es por lo anterior que la Corte Suprema revoca la sentencia apelada y en su lugar, acoge el recurso de protección interpuesto, ordenando al Banco Scotiabank Chile que desinforme la deuda que mantiene con la recurrente derivada del Contrato de Apertura de Línea de Crédito para Estudiantes de Educación Superior con Garantía del Estado, que fue declarada prescrita y, se oficie a la Comisión para el Mercado Financiero, para que elimine, en forma inmediata, la publicación de la deuda antes individualizada.

En base a los tres casos expuestos, es que reiteramos la idea inicial, donde el uso de las redes sociales y el tratamiento no consentido de estos mismos datos puede transformarse en un arma de doble filo. Por un lado, tenemos que las "funas" constituyen un acto de autotutela, a través del cual las personas entienden que en ellas está el tomar la justicia por sus propios medios, aspecto que está sumamente proscrito en nuestro ordenamiento jurídico y ante ello, nuestros Tribunales de Justicia se han pronunciado, en que "nadie tiene el derecho de juzgar y condenar

por sí mismo, mediante una imputación imposible de refutar, y además de amplia difusión, hechos seriamente reprochables a nivel social y penal"[21], puesto que, a contrario sensu, se admitirán acusaciones carentes de fundamento y sin un proceso previo y justo. Y, por otro lado, no es posible que estando a nivel país a vías de desarrollo de la tecnología se admita la exposición de nuevos riesgos, tales como el facilitar la recolección y tratamiento de los datos personales de los usuarios, sobre todo para efectos de comercializarlos sin su consentimiento por parte de agentes de comercio y sin algún organismo u autoridad que fiscalice dichos actos.

3) Desarrollo de la legislación "electrónica" en Chile en relación a los datos personales

Como bien se hizo mención, en el desarrollo de la protección de los datos personales en nuestro país se tuvo como primer acercamiento a nivel legal en la Ley Nº19.628, que fue debidamente promulgada y publicada en el Diario Oficial, siguiendo los artículos 6 y 7 del Código Civil con fecha de veintiocho de agosto de mil novecientos noventa y nueve, la cual tiene por título "Sobre la Protección de la Vida Privada", regulando por tanto el derecho a la protección de datos personales.

Al momento de presentar dicho proyecto de ley, nos encontrábamos muy atrasados con respecto a otros países. El proyecto de ley fue inspirado por la normativa de España, Francia, Reino Unido, Noruega, legislaciones que datan entre las décadas de los años 70 y 80. A medida que el proyecto se tramitaba, fue tomando relevancia el texto de La Ley Orgánica 5/1992 sobre regulación del tratamiento automatizado de los datos de carácter personal de España, pudiendo llegar a considerarse la ley N°19.628 tributaria de esta. Por lo anterior fue que la moción aprobada por el Senado fue muy completa al intentar proteger la vida privada en su totalidad, pero luego de 6 años de tramitación, el proyecto original terminó reducido a una ley que protegió específicamente los datos personales y de manera insuficiente; como hemos visto en el capítulo anterior no es una ley que abarque todo el espectro que conlleva este derecho y lo anterior lo podemos fundamentar con lo expuesto por el profesor Felipe Vial Claro que señala:

> Tal como el proyecto fue definitivamente aprobado por el Poder Legislativo y contrariamente a lo que su título sugiere, la ley no regula orgánicamente todos los aspectos de la vida privada de las personas, entre los que podrían haber quedado comprendidas materias tales como la violación de domicilio, la violación de la correspondencia, la interceptación de las comunicaciones y, en general, la protección del honor, la imagen y la intimidad de las personas. Por el contrario, la norma regula de una manera muy específica el tratamiento de los datos de carácter personal en registros o bancos de datos (art. I). La ley protege la vida privada de las personas naturales en cuanto ésta puede verse afectada por la recolección, registro, procesamiento, comunicación o utilización que se haga de cualquier forma, manual o automatizada, de

[21] (Sentencia Corte de Apelaciones de Valparaíso, Sala Primera, Rol Nº130178-2022, de 28 de diciembre de 2022)

> sus datos personales, en registros o bancos de datos, por parte de personas u organismos públicos o privados.[22]

De la cita expuesta y continuando con la idea, concordamos con el profesor debido a que solo tuvo a la vista un ámbito en concreto, por lo que en consecuencia podemos señalar que ya hace más de veinte año nuestros juristas y profesores de derecho plantean que esta ley tuvo que tener una mayor extensión para prever otras situaciones jurídicas con respecto a este derecho de protección de datos personales por vía electrónica, ya que paralelamente a la dictación de la ley, la sociedad estaba experimentando un cambio tecnológico como no se había visto con anterioridad y como señalamos en el capítulo uno en el segundo apartado tomó bastante relevancia los datos personales, ya que no solo habían instituciones financieras capaces de obtener datos sensibles de los ciudadanos, ya que el internet ya estaba llegando a nuestro país y en un periodo corto de tiempo cada ciudadano era capaz de acceder a esta.

En razón de lo anteriormente mencionado es que la ley en cuestión se quedó atrás desde su entrada en vigencia y actualmente es la jurisprudencia a través de las acciones de protección interpuesto a nuestros tribunales superiores de justicia quienes se han hecho cargo de llenar este aspecto interpretando el artículo 19 N°4 de forma amplia para abarcar estas situaciones que se han estado dando, ya que en el presente año 2023 la Ley Nº19.968 no ha sido tomada en consideración por los legisladores para dar una mayor resguardo al derecho de protección de datos personales. En este punto pasaremos a revisar los artículos más relevantes de la ley sobre la protección de la vida privada, ya que es la regulación especial atingente a la protección de datos personales después de nuestra Constitución de la República de Chile.

En el Título preliminar se establecen las definiciones y lo que ha de entenderse como ha de entenderse el tratamiento de datos personales; que a su vez el Título I abarca la utilización de los datos personales. El Titulo II de la Ley N°19.628, llamado de "*los derechos de los titulares de los datos",* en su artículo 12 dispone una serie de derechos comunes para los titulares de los datos, de los cuales podemos hacer mención del derecho de Acceso, de Rectificación o Modificación, de Cancelación y de Oposición o Bloqueo. En este momento es posible señalar que esta autodeterminación informativa fue recientemente incorporada a través de la reforma a la Constitución Política de la República en 2018 por la Ley Nº21.096 de forma implícita al resguardar el derecho a la protección de datos personales contenidos en el artículo 19 N°4 y que nos remite justamente a este apartado de la legislación electrónica y para entender qué es esta figura es que citamos al Jurista Pablo contreras quien señala lo siguiente:

> Es necesario, al menos someramente, explicar el concepto y fundamento de la autodeterminación informativa. En términos simples, la autodeterminación informativa se ha entendido como el "control que ofrece a las personas sobre el uso por terceros de información sobre ellas mismas"63. El rasgo de autodeterminación como autocontrol es expresión de su fundamento: el libre desarrollo de la personalidad. Normativamente,

[22] (Claro Vial, Felipe. 2001, págs. 23-37)

> garantizar una autonomía decisional respecto de la información personal de un individuo es lo que posibilita el libre desarrollo de la personalidad. Éste es el fundamento de las sentencias del Tribunal Constitucional Federal alemán, revisadas en la sección En efecto, la cláusula constitucional de dignidad, entendida en su dimensión de autonomía , obliga al Estado a tratar a los miembros de la comunidad política como personas capaces de autodeterminarse, entre otras cosas, en el uso de su información personal, con el objeto de que puedan programar su propio plan de vida. En otros términos, tratarlas como fines en sí mismos. Por ello, la autodeterminación informativa garantiza "la facultad del individuo de decidir básicamente por sí sólo sobre la difusión y utilización de sus datos personales". Esto impide la instrumentalización de las personas y reducirlas a meros medios para alcanzar fines privados o estatales"[23]

Antes de entrar al Habeas Data propiamente tal, debemos tener presente que es una acción de rango legal por lo que se interpone ante un tribunal de letras en lo civil y esto genera problemas debido a que estamos haciendo alusión a una garantía constitucional que se puede ver vulnerada y requiere una solución con la mayor celeridad posible y esta acción no resulta eficaz para solucionar los problemas que se pueden presentar y lo anterior lo podemos fundamentar con lo señalado por el profesor Pablo Contreras, quien dice lo siguiente:

> Tal como en su momento lo evaluó la Cámara de Diputados, el procedimiento actual de Habeas Data establecido en la Ley Nº19.628 no es eficaz para proteger los derechos de las personas, ya que "el titular de los datos tiene derecho a recurrir al juez de letras en lo civil del domicilio del responsable", lo que "implica un costo para el afectado y un tiempo de tramitación considerable que no se ajusta a las exigencias de los actuales sistemas de información.*[24]*

Por lo tanto, la vía principal para ejercer los derechos contemplados en esta ley y la CPR en Chile es el Habeas Data que es una acción cautelar de rango legal derivada del Habeas Corpus, que en las modernas sociedades de la información permite a los titulares de los datos personales y patrimoniales "autodeterminar" el uso que se haga de sus antecedentes cuando ellos son recopilados, registrados y cruzados computacionalmente. El Habeas Data actúa sobre la autodeterminación informativa, ya sea que lo haga de manera judicial o extrajudicial el titular de los datos. Las causales de procedencia del Habeas data, están contenidas en el artículo 16 de la ley de datos personales. El sujeto activo de tal acción es el titular de los datos personales y debe dirigirse contra el responsable del banco de datos sea organismo público o privado que denegó algún derecho o ha realizado tratamiento indebido de aquellos y en consecuencia de loa anterior es que los fundamentos para que sea procedente son los siguientes:

En primer lugar, si el responsable del registro o banco de datos no se pronunciara sobre una solicitud de información, modificación, bloqueo, cancelación o eliminación de datos personales dentro de dos días hábiles. En segundo lugar, si el responsable del registro o banco de datos denegare una solicitud de información, modificación, bloqueo, cancelación o eliminación de

[23] (Contreras, Pablo. 2020, pág. 101)
[24] (Contreras, Pablo. 2020, pág. 113)

datos personales por una causa distinta de la seguridad de la Nación o el interés nacional. En tercer lugar, si el responsable del registro o banco de datos denegare una solicitud de información, modificación, bloqueo, cancelación o eliminación de datos personales por motivos de seguridad de la Nación o el interés nacional. En cuarto lugar, con la modificación introducida por la Ley N°19.812 , también se puede reclamar a través de este procedimiento por infracción a los artículos 17 y 18 de la Ley Nº19.628, que regulan la forma y los plazos en que pueden comunicarse a terceros por los responsables de los registros o bancos de datos de carácter económico, financiero, bancario o comercial.[25]

Ahora bien, dichas causales no dotan de una taxatividad, puesto que también se considera el artículo 19 N°4 inciso final de la Constitución Política de la República, dado que su infracción otorga la vía de acción contemplada en esta norma, por lo que en consecuencia no se trata de requisitos copulativos, ya que basta con encasillar la infracción a una causal para que sea procedente. Las sanciones que contempla la ley se traducen, en primer término, en una multa de diez a cincuenta unidades tributarias mensuales en el caso que se infrinja lo dispuesto en los artículos 17° y 18°, es decir las normas especiales respecto a los datos económicos, financieros, bancarios y comerciales; y multa de una a diez unidades tributarias mensuales en todos los otros casos. En el caso de la falta de entrega oportuna de la información o el retardo en efectuar la modificación, el juez podrá aplicar una multa de dos a cincuenta unidades tributarias mensuales y si el responsable de datos fuere un organismo público el tribunal podrá sancionar al jefe del servicio con la suspensión de su cargo, por un lapso de cinco a quince días.[26]

Asimismo, seguida de la sanción mencionada anteriormente, el artículo 23 agrega la "Responsabilidad del banco de datos personales" por los daños patrimoniales y morales que fuesen causados por el tratamiento indebido de los datos aludidos, pudiendo fijar el juez el monto de la indemnización de perjuicios de ser requerida por el afectado que lo solicite al tribunal. La acción de indemnización de perjuicios puede conocerse en forma conjunta con el Habeas Data, sin perjuicio de lo establecido en el artículo 173 del Código de Procedimiento Civil. En razón de lo anterior es que podemos preguntarnos la naturaleza jurídica sobre la responsabilidad que tienen las instituciones que la ley alude, se ajusta a lo que en derecho civil se conoce como "responsabilidad extracontractual", ya que si bien existe una relación jurídica entre los particulares por medio de un contrato esto es excepcional (responsabilidad contractual), ya que la ley apunta a una figura más amplia porque la fuente de responsabilidad en este caso es la ley y por tanto se alude a la primera figura jurídica que acabamos de hacer alusión.

En base a lo anterior es que hay que señalar quién debe probar la infracción, es decir, se presume por culpa o dolo como sucede en materia civil o debe ser probada por la víctima, en consecuencia debemos tener presente que la ley si bien utiliza la expresión "indebido" para referirse a la responsabilidad que nace por la vulneración de los datos personales, se relaciona con la culpa y como señalamos en el punto anterior se encuentra vinculada a la responsabilidad extracontractual por lo que se debe aplicar la regla general contemplada en el artículo 1698 del

[25] (Ministerio Secretaría General de la Presidencia, 1999. Ley Nº19.628. Artículos 16,17,18,19)
[26] (Ministerio Secretaría General de la Presidencia, 1999. Ley Nº19.628)

Código Civil que señala que: “Incumbe probar la existencia de las obligaciones o la extinción a quien alega aquéllas o ésta.”[27]

Para concluir con este apartado debemos mencionar que el Habeas Data es una acción sumamente importante para la sociedad, dado que como hemos mencionado anteriormente es la vía idónea para proteger los datos personales de las personas naturales en materia electrónica dado el desarrollo acelerado que estamos presenciando de la tecnología y lo previamente expuesto es en teoría, ya que en la práctica se mantiene muy acotado su aplicación por lo breve que resulta la ley siendo la única que regula en específico este tema.

[27] (Ministerio de justicia, 2023, Código Civil, pág.390)

CAPÍTULO 3

SIMILITUDES Y DIFERENCIAS ENTRE AMBOS ORDENAMIENTOS, RESPECTO AL ACCESO DE DATOS PERSONALES

1) El objetivo de Alemania en relación al derecho de protección de datos personales en la actualidad

Como se ha explicado en los puntos anteriores, Alemania ha sido uno de los primeros países que ha puesto en la palestra conceptos y términos en su propia legislación acerca de la protección de los datos personales, esto desde 1970 mediante la Ley "Datenschutz", la cual ha estado en una constante evolución, para que dicha norma jurídica no se quede obsoleta y pueda desarrollarse a la par de la sociedad y la propia globalización. Esto por medio de la Ley Federal de Protección de Datos de la República Federal Alemana de 1977, la sentencia del Tribunal Constitucional Federal de Alemania en la cual se declara inconstitucional algunos preceptos de la Ley de Censo en 1983, también por la nueva Ley de Protección de Datos Personales de 1990 y posteriores actualizaciones como la del año 2017. Teniendo entonces un gran trabajo preparatorio para cumplir con sus metas.

Alemania dentro de sus Leyes de Protección de Datos que ha tenido a lo largo de la historia, siempre tuvo una finalidad en común, la cual es la protección a la persona, en el sentido más amplio posible, pero facilitando el derecho a su autonomía o autodeterminación, entregando ciertas restricciones y derechos sobre los propios datos personales, como también protección a los ciudadanos del uso no autorizado de los mismos. Pero siempre asegurando la autonomía de la persona.

Un gran objetivo que tiene Alemania en torno a la protección de los datos personales es poder aumentar y fomentar la participación ciudadana en torno a la toma de decisiones relacionadas con la protección de estos datos, en donde se involucre a organizaciones no gubernamentales, empresas y los propios ciudadanos a generar instancias de debate, esto para concientizar a la sociedad sobre sus derechos y deberes y la importancia que tienen en la protección sus datos. Todo lo anterior para promover la transparencia y la rendición de cuentas sobre los datos personales.

En relación a lo anterior, se creó la Asociación Alemana para la Protección de Datos, esta es una organización registrada sin fines de lucro, la cual fue fundada en 1977 en Bonn, presidida por Frank Spaeing en la cual cuentan con 240 miembros, esta se encarga de asesorar y educar a la población sobre los peligros del uso del procesamiento electrónico de datos y las posibles restricciones al derecho a la autodeterminación informativa. Esta asociación cuenta con la creación de un DVD, este trata sobre muchos temas relacionados con la protección de datos, ya sea, en el internet, para la protección de datos de consumidores, para la protección de datos de los empleados, etc.

Así evalúan su propio trabajo la propia Asociación Alemana para la Protección de Datos:

> Incluso casi 40 años después de la "sentencia censal" del Tribunal Constitucional Federal ("derecho a la autodeterminación informativa") y mucho después del novedoso escenario "1984" de Orwell, la protección de datos aún no es un derecho civil evidente e inatacable.
>
> En cambio, el uso masivo y estrechamente interconectado de la tecnología de la información aparece como una panacea para resolver muchos problemas sociales.
>
> Vemos como una amenaza a nuestros valores democráticos básicos que los derechos personales de los individuos tengan cada vez más prioridad sobre los supuestos intereses de seguridad.[28]

Es por esto que Alemania se ha esforzado en educar a la población sobre la importancia de la privacidad y la protección de datos, esto por medio de campañas de concientización pública como lo es el "Data Protection Day", el cual se celebra cada 28 de enero, esto basado en la fecha en la que se firmó el convenio de protección de datos del Consejo de Europa, mejor conocido como el Convenio 108, siendo este el único instrumento internacional, multilateral y legalmente vinculante para proteger la privacidad y los datos personales. En este "Data Protection Day" se realizan actividades para generar conciencia de dichos datos, dirigiéndose a un público general, como profesores, estudiantes e incluso conferencias en empresas. Estas campañas son bastante importantes, ya que, los datos personales se procesan en cada momento, ya sea, en el trabajo como también en las búsquedas o navegaciones por Internet, y generalmente las personas ignoran los riesgos relacionados a la protección de los datos personales, más aún con la explosión de las redes sociales.

En este mismo sentido, Alemania desde el año 2017 ha introducido gradualmente la educación de los datos personales como tema obligatorio en las escuelas. Con relación a esto, Alemania tuvo un problema en torno al programa Office 365 de Microsoft con las escuelas. Microsoft Office 365 es una herramienta creada en Estados Unidos, la cual permite crear y compartir diferentes documentos de las aplicaciones de la empresa Microsoft, como, por ejemplo: Word, Excel, PowerPoint, etc., en donde se puede acceder a todas estas aplicaciones en tiempo real, desde cualquier dispositivo que tenga acceso a Internet, además también puede tener acceso al correo electrónico, mensajería, almacenamiento en la nube, entre otros.

Es por lo anterior que la Conferencia Alemana de Protección de Datos emitió una declaración de la imposibilidad de poder utilizar dicha aplicación en las escuelas alemanas. Esto debido a que se halló una falta de transparencia en lo que respecta a la protección de datos y el posible acceso de terceras personas. Incumpliendo entonces las leyes de protección de datos.

La declaración de la Conferencia Alemana de Protección de Datos dictaminó lo siguiente:

> Los controladores deben ser capaces de cumplir con sus obligaciones de responsabilidad de acuerdo con el Art. 5 (2) GDPR en todo momento. Cuando se utiliza Microsoft 365,

[28] Deutsche Vereinigung für datenschutz e.V.. *Datenschutz Nachrichten*. Recuperado de https://www.datenschutzverein.de/vereinsprofil/

> todavía se pueden esperar dificultades en este sentido sobre la base del "suplemento de protección de datos", ya que Microsoft no revela completamente qué operaciones de procesamiento tienen lugar en detalle. Además, Microsoft no revela completamente qué operaciones de procesamiento se llevan a cabo en nombre del cliente o cuáles se llevan a cabo para sus propios fines. Los documentos contractuales no son precisos a este respecto y no permiten evaluar de forma concluyente el tratamiento, que puede ser incluso amplio, incluso para fines propios de la empresa.
>
> El uso de datos personales de los usuarios (por ejemplo, empleados o estudiantes) para fines propios del proveedor excluye el uso de un procesador en el sector público (especialmente en las escuelas).[29]

Siendo el principal problema que las autoridades estadounidenses podrían acceder a los datos almacenados en la nube sin que Alemania tenga control de ello.

Por otro lado, Microsoft respondió a dicha declaración señalando lo siguiente:

> M365 no solo cumplen, sino que con frecuencia mejoran, las estrictas leyes de protección de datos en la UE. Nuestros clientes en Alemania y en la UE pueden seguir utilizando los productos M365 sin dudarlo y de manera segura y legal.
>
> Los productos Microsoft 365 cumplen los estándares del sector más estrictos en lo que se refiere a privacidad y seguridad de datos. Estamos respetuosamente en desacuerdo con las preocupaciones planteadas por la Datenschutzkonferenz y ya hemos implementado muchos de los cambios sugeridos a nuestros términos de protección de datos. Seguimos comprometidos con el trabajo con la DSK para abordar cualquier preocupación que sigan teniendo.[30]

Considerando ambas declaraciones, el Comisario de Datos de Hesse concluyó que el tratamiento de datos de parte Microsoft es ilegal, que la protección de los datos de los niños que van a las escuelas alemanas es más importante, y que se destaca que la empresa Microsoft ha sufrido bastante en torno a hackeos, por lo que, los datos que puede contener en la nube están en peligro, por lo tanto, se declaró la imposibilidad de volver a utilizar Office 365 de Microsoft en las escuelas.

Como se ha mencionado en puntos anteriores, uno de los objetivos claves de Alemania en torno a la protección de datos personales es la adaptación a las tecnologías emergentes y su impacto en la privacidad de los datos. A medida que la tecnología continúa avanzando y transformando la forma en que las empresas y los individuos recopilan, procesan y utilizan datos personales,

---

[29] (Tutanota (2022). *El Office 365 de Microsoft se declara ilegal para las escuelas alemanas, ¡otra vez!*. Recuperado de: https://tutanota.com/es/blog/posts/microsoft-office-365-email-alternative.)

[30] (MCPRO (2022). *Problemas para Microsoft 365 por la RGPD: prohibido en las escuelas en Alemania*. Recuperado de https://www.muycomputerpro.com/2022/12/01/microsoft-365-rgpd-prohibido-escuelas-alemania.)

es necesario garantizar que las regulaciones y leyes de protección de datos también evolucionen para reflejar estas nuevas realidades y no quedar estancados en el pasado.

En este sentido, se han hecho bastantes actualizaciones a su Ley Federal de Protección, incluyendo disposiciones específicas sobre tecnologías emergentes, como el procesamiento automatizado de datos y la inteligencia artificial, esto para cumplir con las exigencias y tener concordancia con el Reglamento General de Protección de Datos de la Unión Europea, dicho reglamento contiene medidas esenciales para fortalecer los derechos fundamentales de las personas en la era digital y su protección de datos.

Alemania ha tenido inconvenientes con empresas de tecnologías emergentes por el no cumplimiento a las disposiciones del Reglamento General de Protección de Datos. Uno de los ejemplos es que el Comisionado Federal de Protección de Datos Alemán solicitó a la Oficina Federal de Prensa, que dirige la página de Facebook del Gobierno Federal Alemán que deje de operarla. Esto en base a una investigación en donde se identificó que el tratamiento y recopilación de datos que se informaba no era aplicable a una página de un organismo público y que dicha Oficina Federal de Prensa no sabía qué uso se hacía de los datos recopilados.

En este mismo sentido, se le acusó a las diferentes redes sociales como por ejemplo Facebook, Instagram, WhatsApp y Twitter de recabar información de los datos personales de sus usuarios sin su conocimiento. Esto mediante una investigación de la autoridad alemana, en donde se restringió la recopilación y el procesamiento de los datos de los usuarios de dichas redes sociales. Alemania pide prohibir el uso del botón de "Me Gusta" de Facebook, ya que, este permite recabar información sobre los usuarios cuando navegan en redes ajenas sin que se den cuenta. Emitiendo así una orden para evitar que Facebook recopile datos personales de los usuarios en Alemania por parte del Comisionado de Hamburgo.

Por su parte, Facebook explicó que esa investigación realizada da una imagen inexacta y que ellos no poseen una posición dominante en Alemania ni en ningún otro país, en donde además señaló su plan en un comunicado, el cual es continuar el diálogo y ayudar a entender mejor los procesos actuales y cómo éstos respetan la privacidad de los usuarios de internet alemanes, rechazando firmemente cualquier afirmación que señale que Facebook no cumple con los estándares de protección de datos de la Unión Europea.

Otra tecnología emergente es la inteligencia artificial, la Real Academia Española la define de la siguiente manera: "Disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico"[31]

En torno a esta se han desarrollado bastantes herramientas como lo es el "ChatGPT", el cual es un chatbot inteligente que ayuda a automatizar tareas, buscando proporcionar respuestas al usuario a través del chat mediante un aprendizaje automático.

[31] (Real Academia Española (RAE): *Diccionario de la lengua española*, 23.ª ed. Recuperado de https://dle.rae.es/inteligencia#2DxmhCT.)

Alemania inició una investigación sobre el uso de los datos personales que hace el chatbot antes mencionado, enviando un cuestionario a "OpenAI", empresa creadora de dicho chat. Marit Hansen, jefa del Centro Estatal Independiente de Protección de Datos, explica que están pidiendo dicha información para verificar que dicho chatbot se encuentra bajo el alero del Reglamento General Europeo de Protección de Datos, poniendo un plazo de hasta el día 11 de junio de 2023 para tener una respuesta. Hasta el momento, la Unión Europea se encuentra estudiando la situación e ideando una forma de aplicar de forma conjunta la ley de protección de datos. Destacando que países como Italia ha decidido bloquear dicha herramienta.

Finalmente, otro de los objetivos principales de Alemania en torno a la protección de datos personales es promover la protección de datos en el contexto global, la globalización ha generado una necesidad de establecer normas y regulaciones internacionales para garantizar la protección de los datos personales en todo el mundo.

Una de estas medidas es la promoción de la cooperación internacional en la protección de datos personales. Alemania ha establecido acuerdos de cooperación con otros países y organizaciones internacionales para compartir información, conocimientos y experiencias sobre la protección de datos. Esto incluyendo lo mencionado anteriormente en torno a la concordancia de la Ley de Protección de Datos Personales con el Reglamento General de Protección de Datos de la Unión Europea.

En este sentido, la Ministra de Estado, Dorothee Bär firmó una declaración conjunta de cooperación en la construcción de un ecosistema de identidades digitales entre Alemania y España. Esto por medio de la tecnología "Self-sovereign Identity (SII)". En la propia declaración se señala lo siguiente:

> La identidad digital (es la capacidad de hacer afirmaciones sobre su identidad o atributos para acceder a información pública y servicios privados en un espacio digital) es un componente fundamental en el mundo actual. Muchas interacciones digitales, y especialmente las que son más relevantes, como el trato con las autoridades públicas, el uso de la banca por Internet o la compra en línea, requieren que las partes puedan identificarse entre sí de manera confiable y compartir información de identidad entre ellas de una manera segura y confiable.
>
> Por lo tanto, la identidad digital constituye la capa fundamental sobre la cual los servicios digitales, tanto públicos como privados, se puede proporcionar a nuestros ciudadanos, quienes deben estar facultados para compartir de forma segura sus propios datos de identidad bajo su control exclusivo. Es una de las palancas más importantes de los Estados miembros europeos y de la Unión Europea en su conjunto tenemos que aprovechar el potencial de nuestras economías y el mercado único europeo en un mundo digital.[32]

[32](Bär, D., & Artigas, C. 2021)

En síntesis, la tecnología "Self-sovereign Identity" pretende devolver el poder de la identidad al propio usuario, permitiendo así, compartir de forma segura sus propios datos personales, protegiendo dichos datos y rigiéndose al propio Reglamento General de Protección de Datos de la Unión Europea. Destacando la posibilidad de que otros Estados se unan a dicha cooperación y se logren mejores resultados y mejorar la protección de datos personales en estos diferentes Estados.

Concluyendo que todos estos objetivos mencionados de Alemania en torno a la protección de datos personales buscan permitir a los usuarios tener un control completo sobre sus datos personales, generando una protección de la privacidad de los usuarios en línea y garantizar que sus datos personales estén seguros en el entorno digital.

2) La finalidad de Chile en relación al derecho en estudio y su conexión con el derecho a la honra y a la privacidad en la actualidad

Al efecto, hay que señalar que la Constitución Política de la República chilena contempla este derecho en las garantías fundamentales consagradas en el artículo 19, en particular en su numeral 4 inciso segundo junto al derecho de protección a la vida privada y a la honra, punto que ahondaremos más adelante. Además, es menester señalar que este artículo nos remite a la Ley de Protección de Datos, legislación que tiene por objeto garantizar el derecho a la privacidad y proteger los datos personales de las personas físicas, aplicando dichas disposiciones a su vez en el tratamiento de los mismos realizado por todos los contribuyentes, particulares, empresas y organizaciones.

En razón de ello, el derecho a la protección de los datos personales, en doctrina, se distingue del derecho a la intimidad, puesto que el primero impone deberes jurídicos a terceros para hacer efectiva la reserva de información y control de datos, mientras que el derecho a la intimidad se trataría de una garantía que tiende a excluir a terceros de la esfera personal de cada uno de nosotros, sin imponer obligaciones jurídicas sobre ellos, salvo de no traspasar nuestra privacidad. Al respecto, para algunos, este derecho constituye uno de carácter fundamental en nuestra Carta Magna, siendo por ende ambos derechos diferentes en su contenido, no obstante nuestros legisladores, al momento de incorporar la protección de datos personales dentro del artículo 19 Nº4 de nuestra Constitución Política, lo comprendieron como un derecho que nace o tiene una relación directa con la garantía constitucional que ampara la honra y la privacidad, dado que, como bien señala el profesor Pablo Contreras a propósito de las discusiones parlamentarias en torno a la reforma constitucional que incorpora este derecho; el académico argumentó lo siguiente:

> En primer lugar, los debates legislativos dan cuenta que la razón de ubicar sistemáticamente a la autodeterminación informativa en el art. 19 No. 4 de la Constitución se basaba en la conexión –no del todo aclarada– con el derecho al respeto y protección de la vida privada o, derechamente, con la intimidad. En efecto, como se lee en diversos apartados de la tramitación legislativa, el derecho a la protección de datos personales se entendió como una "dimensión moderna" del derecho a la

> protección de la vida privada. En este sentido, algunos incluso plantearon que la privacidad era un "derecho madre" respecto de la autodeterminación informativa y por ello se justificaba "anclar" al segundo en la norma del primero[33]

Ahora bien, teniendo en cuenta lo expuesto en los capítulos anteriores, la finalidad perseguida por nuestro ordenamiento jurídico sobre la protección de datos personales es la misma que el derecho a la honra y a la vida privada, esto es, proteger el ámbito de la intimidad de las personas naturales y su reputación, conocida esta última como la del "buen nombre" que responde a la percepción que tiene la sociedad frente a terceros, ya que nuestros congresistas estimaron que dicha figura se encuentra envuelta dentro del derecho en comento, pese a ser tratado de forma genérica y sin darle un contenido en el mismo numeral "*protección a la vida privada y a la honra de la persona"***.** Por consiguiente, se entiende que poseen el mismo fin, asimismo porque la Ley Nº19.628 no ha sido modificada de forma extensiva para diferenciar el derecho a la protección de datos personales con la esfera regulada en el artículo 19 Nº4 inciso 1 de nuestra Constitución.

Es más, en el presente año en que se realiza esta investigación aún se entiende en nuestro marco jurídico que ambos derechos son lo mismo sin distinción, ya que nuestros legisladores no han mostrado interés en diferenciarlos en la propia carta magna o en la misma ley que se remite este artículo 19 Nº4 que las trata en conjunto, esto teniendo en consideración los debates finales que se sostuvieron en su momento para dictar la ley de reforma.

A raíz de lo anterior, es que nos lleva a la necesidad de traer a colación el comento de las sesiones de la comisión redactora de la reforma de la Ley Nº19.628 por medio de la Ley Nº21.096. En sus inicios, se plantearon una diferencia entre ambos derechos en los términos expuestos en acápites anteriores, es decir, se encuentran ambos derechos vinculados pero son autónomos e independientes entre sí, ya que la finalidad perseguida por la consagración de este derecho de la protección de datos personales en nuestra Constitución era, en principio, que los datos almacenados fueran completamente manejados por su titular o dueño para exponer lo que estimara conveniente a los demás miembros de la sociedad, respetando con ello lo que las leyes designan al respecto lo anterior lo fundamentamos en lo que fue el texto de la moción por parte de los legisladores que fue la siguiente:

> Art. 19: La Constitución asegura a todas las personas: […] No. 4. El respeto y protección a la vida privada y a la honra de la persona y su familia. Toda persona tiene derecho a la protección de sus datos personales y obtener su rectificación, complementación y cancelación, si estos fueren erróneos o afectasen sus derechos, como asimismo a manifestar su oposición, de acuerdo con las disposiciones establecidas en la ley. Su tratamiento sólo podrá hacerse por ley o con el consentimiento expreso del titular; […][34]

[33] (Contreras, Pablo. 2020, pág. 100)
[34] (Contreras, Pablo. 2020, pág. 103)(HDL)

Con ello, ya se planteaba en las sesiones que se debía realizar una reforma a la Ley Nº19.628 de forma secuencial a la reforma constitucional, lo cuál a día de hoy no se ha plasmado, entendiendo además que en esta reforma en un principio se le daría preeminencia a la autodeterminación informativa con el fin de despejar dudas con respecto al mecanismo de protección de este derecho, ya que como hemos planteado anteriormente, el particular cuenta con dos acciones, la acción o recurso de protección y la acción Habeas Data. En relación a lo anterior es que al final esto último quedó implícito con la propuesta final de la reforma constitucional al incorporar al artículo 19 Nº4 la protección de datos personales.

En este punto haremos algunas distinciones que existen entre ambos derechos que han sido tomadas en cuenta por la jurisprudencia y doctrina constitucionalista, puesto que como hemos hecho mención previamente, el legislador en definitiva les dio el mismo tratamiento a ambos. A continuación, pasamos a revisar y comentar sus diferencias.

En primer lugar, en cuanto a las acciones, el particular ante una infracción o vulneración de las garantías, recurren a la acción constitucional de protección como vía de reparación y restauración del imperio del derecho, mientras que, si hablamos dentro del plano en que la persona ha sido lesionada en sus datos personales, cuenta además con la acción Habeas Data que nace a partir de la Ley Nº19.628 y que hemos mencionado en varias ocasiones en esta investigación. No hay duda alguna que, con respecto al derecho a la vida privada y la honra, la vía sin discusión por la jurisprudencia y doctrina es la acción constitucional de protección, la complejidad recae con respecto al segundo derecho, debido a que, según lo reglamentado por nuestra Carta Magna, la acción de protección se entiende como el medio idóneo para enmendar la vulneración del derecho fundamental en estudio. Y en efecto, la jurisprudencia y la doctrina se encuentran divididas, sosteniendo parte de la primera que precisamente dado a que esta garantía tiene su regulación en una ley y que esta misma establece la acción de Habeas Data, no hay que despejar más puntos en duda, pero algunos autores entienden que viene del particular el optar por dicha vía o por la acción constitucional de protección, amparándose bajo el fundamento de que se trata de una ley especial que contempla esta situación jurídica, siendo al final la persona que elija a su arbitrio la acción más conveniente para obtener una reparación integral del daño causado.

En segundo lugar, es preciso mencionar una diferencia entre ambos derechos y es que el derecho a la protección de la vida privada tiene un carácter eminentemente extrapatrimonial, esto es, no avaluable en dinero, a menos que sea vulnerado y sea susceptible de una reparación por medio de la indemnización de perjuicios por daño moral. Es decir, mientras no sé realice una infracción a este derecho se mantiene como uno que no tiene un valor nominal y lo anterior se fundamenta en una sentencia del Tribunal Constitucional que señaló lo siguiente:

> El derecho a la honra, por su esencia espiritual y moral como emanación de la dignidad de la persona humana, carente de materialidad, no posee en sí mismo valor económico o patrimonial. El resultado dañino de los atentados en su contra se traducirá, por regla general, en sufrimientos o mortificaciones de igual carácter, esto es, en daño moral".(STC 1185, c. 16)[35]

A su vez, el Tribunal Constitucional ha sostenido que es procedente la demanda por daño moral y lo ejemplificamos con el subsiguiente criterio de la corte:

> La exclusión del daño moral por vulneración al derecho a la honra es arbitraria. Resulta arbitraria toda vez que impide siempre la indemnización del daño moral por vulneración al derecho a la honra, afectando, por tanto, el derecho constitucional en su esencia (STC 1679, c. 15) (En el mismo sentido, STC 1798, c. 13; STC 1419, cc. 25 y 29).
>
> La exclusión del daño moral por vulneración al derecho a la honra es desproporcionada. En cuanto impide a priori y de forma absoluta cualquier indemnización por daño moral sin considerar excepción alguna ni permitir que el juez pueda determinar su procedencia (STC 1679, c. 16) (En el mismo sentido, STC 1419, c. 31; STC 1463, c. 31; STC 1741, c. 14; STC 1798, cc. 12 y 14).
>
> Indemnización del daño moral por vulneración a la honra. Las normas del derecho chileno, permiten concluir que el daño causado a la honra por expresiones injuriosas contra una persona es susceptible de indemnización por daño moral cuando éstas, además, califiquen como delito (STC 1463, c. 29)[36]

En consecuencia, y a diferencia del derecho a la vida privada, la protección de datos personales tiene un carácter patrimonial debido a que estos datos son susceptibles de ser apreciable en dinero por las entidades que manejan esta información, ya que tiene una relación directa con el mundo jurídico financiero y, por tanto, la infracción o vulneración de este derecho, da acción para no solo exigir que se rectifique, modifique o excluya información, sino que también puede reclamar la pertinente indemnización de perjuicios. A contrario sensu, lo que ocurre con el derecho a la vida privada y la honra, estos se circunscriben, por regla general, al daño moral, por lo que en la esfera que estamos planteando, podrá además exigir que se le repare el daño tanto emergente como el lucro cesante que se encuentran en nuestro Código Civil, ya que estas entidades o instituciones responden por responsabilidad extracontractual según revisamos previamente.

En tercer lugar, su fundamento jurídico es distinto, como expusimos anteriormente en el capítulo 1 se trata de dos derechos diferentes, que tienen similitudes, pero grandes diferencias que le dan este carácter de autónomo e independiente con el contenido en la primera parte del

[35] (Navarro, Enrique. 2011, pág. 143.)
[36] (Navarro, Enrique. 2011, pág. 144.)

artículo 19 Nº4 y en consecuencia hemos estado revisando en este apartado está distinción se plantea debido a que la protección de datos personales tiene como premisa que el titular tenga un poder de control sobre sus datos para usar y disponer de ello según le parezca acorde, esto sin duda teniendo en consideración las limitaciones a las que pueda verse expuesta por ley; el planteamiento recién señalado es teniendo en consideración, las sentencias del Tribunal Constitucional Federal Alemán y Español .[37]

Por otro lado, el derecho a la vida privada y a la honra se desdobla en dos, debido a que la vida privada tiene por eje central que ninguna persona puede entrar al ámbito personal de un individuo de la sociedad, tanto física como psicológicamente; en cambio, la honra es el prestigio o valor de una persona frente a los demás miembros en primer lugar de su familia y en segundo la sociedad, esto se sustenta en dos sentencias de nuestro Tribunal Constitucional que señaló lo siguiente:

> Sentido y alcance del derecho a la privacidad; Es la situación de una persona, en virtud de la cual se encuentra libre de intromisiones de agentes externos y ajenos a su interioridad física o psicológica y las relaciones que mantiene o tuvo con otros. Sin embargo, este derecho puede tener limitaciones legales por finalidades razonables, además de la intromisión estatal justificada en caso de realización de hechos delictivos (STC 1683, cc. 38, 39 y 41).[38]

Con respecto a la honra, ha dicho lo subsiguiente:

> Sentido objetivo del derecho a la honra. La honra alude a la reputación, al prestigio, a lo que las demás personas piensan sobre una persona determinada. (STC 1419, cc. 8, 18 y 20) (En el mismo sentido, STC 1463, c. 14)
>
> Sentido subjetivo del derecho al honor. El honor alude a lo que una persona piensa de sí misma en cuanto a su valor; es la voluntad de afirmar el propio valor o mérito antes los demás (STC 1419, c. 18 y 20) (En el mismo sentido, STC 1463, c. 14)[39]

Por lo que en consecuencia se puede indicar que esta diferencia es esencial, ya que es la base para hacer la distinción entre ambos derechos, dado que si bien están relacionados no son lo mismo. La última diferencia tiene relación con la discriminación anterior, ya que, versa sobre su génesis o del cómo debe ser tratado como derecho fundamental.

En primer término, el derecho a la protección a la vida privada y a la honra, al ser ambos amparados desde la esfera de la Constitución Política de 1980, siendo una gran innovación en dicho momento y propuesta por el ex Presidente de la República Jorge Alessandri Rodríguez,

---

[37] (Sentencia del Tribunal Constitucional Federal Alemán, BVerfGE 27, 1 (1969). Para sus versiones traducidas, véase a Schwabe (2009) (13 STCE 292/2000, fj. 7)

[38] (Navarro, Enrique. 2011, pág. 141)

[39] (Navarro, Enrique. 2011, pág. 143)

fueron objeto de críticas en su día por la prensa y fue vulnerada su honra y prestigio como individuo.

Por contraparte, el derecho a la protección de datos personales tiene su comienzo con la regularización de los datos frente a entidades financieras y estatales; a nivel de derecho comparado este tratamiento nace a mediados del siglo XX a diferencia de nuestro derecho que recién se empezó a legislar a fines de siglo debido al atraso de conocimiento jurídico que provenía de Europa y se tenía en consideración que se trataba de un derecho que nace en la esfera privada del sujeto si bien ambos derechos marcan esta igualdad se empiezan a diferenciar en sus ámbitos de aplicación en virtud de donde nacen, ya que este segundo derecho fundamental se origina a propósito del crecimiento tecnológico que experimenta la sociedad para almacenar datos de las personas y esta distinción es importante frente al primer derecho.

Para cerrar este apartado, debemos tener presente la necesidad de, que el legislador nacional tome muy en consideración los criterios jurisprudenciales y doctrinales, para con ello regular esta materia de forma autónoma en nuestra Constitución Política de la República y que se desprenda del alero del derecho a la vida privada y a la honra, puesto que en los últimos 40 años se ha vivido un cambio tecnológico a una velocidad acelerada y, por lo tanto, se debe tener en cuenta una norma más completa para abarcar la mayor cantidad de situaciones jurídicas con respecto a los datos personales de los individuos de la sociedad.

3) **Singularizar las deficiencias y aspectos positivos de cada uno de los países en comento respecto al amparo y custodia del derecho de protección de datos personales**

Ya hemos hecho mención acerca del tratamiento que este nuevo derecho ha tenido en ambos ordenamientos, junto a sus elementos, particularidades y tipicidad. Y con ello, desprendemos que tanto Chile como Alemania presentan fortalezas y debilidades; asimismo que contienen el complemento y singularidad necesaria respecto a lo que el otro país necesita.

En una primera vertiente, Chile fue el primer país Latinoamericano en adoptar un marco regulatorio en esta materia del derecho a la protección de datos personales, siendo en sus primeros avances una innovación indiscutible dentro del camino del desarrollo en lo que respecta a dicha protección y resguardo. Es más, efectuó la diferencia entre el derecho a la vida privada y el derecho de datos personales, reconociendo a este último su carácter autónomo, pero a la vez relacionado con el primero al referirse ambos a la esfera del individuo y su entorno. Y también es importante mencionar, qué producto de dicha regulación, se establece que el tratamiento y protección de datos hace referencia a que los diversos medios de comunicación quedan sujetos a las disposiciones de esta ley en lo relativo al tratamiento de datos, definiendo además conceptos esenciales en la comprensión y aplicación de las normas sobre protección de datos.

No obstante, si bien contiene un desarrollo tanto constitucional como legal del derecho a la protección de datos personales, la deficiencia radica, generalmente, en no presentar mayor perfeccionamiento y extensión en nuestro ordenamiento jurídico per se, evidenciando por

consiguiente una insuficiencia hacia su garantía y presentando dudas para los usuarios bajo el alero de su entorno sobre el acceso a dichos datos, quienes tienen la facultad última de procesarlos y cómo se efectúa finalmente el mecanismo de control por parte de las personas naturales y jurídicas para sentirse amparadas por el sistema. Es decir, lo que ocurre al fin y al cabo es, que la figura del Habeas Data legal pese a ser una innovación en el derecho en América Latina, no ha sido lograda su confección del todo para cubrir todas sus aristas de protección, debido a que no estamos ante un mecanismo de custodia a priori preventiva y efectiva, sino que más bien posterior, esto es, ya acaecido el daño; y cómo remediarlo.

En el contexto jurídico chileno, naturalmente la preocupación por el resguardo de la vida privada y, consecuentemente, de los datos de carácter personal, fueron, siguen y serán temas de continua regulación normativa, siendo claramente una tarea difícil que un país tenga una legislación a la par con el desarrollo de la sociedad, sobre todo dentro de esta temática del mundo cibernético y de la tecnología. De hecho, infiriendo un poco en la historia fidedigna de nuestro país, el primer intento por reconocer una cierta protección a la esfera privada de las personas, se remonta al Reglamento Constitucional Provisorio de 1812, pasando por textos como las Constituciones de 1833 y 1925, hasta llegar al Acta Constitucional N.º 3 del 11 de septiembre de 1976, coronada como la primera regulación en consagrar la protección a la vida privada de las personas a nivel constitucional y antecedente directo del confeccionamiento de la Carta Magna de 1980; culminándose este recorrido histórico y normativo con la promulgación de la Ley Nº19.628 de 1999, estatuto que surge bajo la pretensión de tutelar la vida privada, pero que luego de un largo y complejo trámite legislativo terminó enfocándose en la protección de los datos de carácter personal.

Y solo casi diez años después, el legislador tomó cartas en el asunto y la iniciativa de promulgar la *"Ley de transparencia de la función pública y de acceso a la información de la Administración del Estado"* (aprobada por el artículo 1º de la Ley Nº20.285 de 2008), también conocida como "Ley de transparencia", el cual tiene por objeto el tratamiento y acceso a la información pública. En este sentido, ambos cuerpos legales regulan la información, pero desde diversas aristas, lo que el primero resguarda la información que concierne a personas naturales identificadas o identificables para garantizar que sean ellos quienes decidan sobre su uso, el segundo tiene por objeto la información que obra en poder de los órganos del Estado (la que puede incluirse dentro del concepto de datos personales) con la pretensión de favorecer su conocimiento por parte de los ciudadanos. Y lo que ocurre es que no se han diferenciado ambos términos, es decir, las nociones de acceso a la información pública y la transparencia en lo público.

Cuando hacemos mención del acceso a la información pública, dentro de la terminología jurídica, se refiere a la facultad que tiene el ciudadano o usuario de acceder a la data que poseen las entidades de índole pública, siendo esta entrada de dos formas; ya sea el “mostrar” sin que se requiera dicha información o bien “permitir ver” o derecho de saber que se manifiesta cuando la persona pide de forma explícita cierta información a un organismo del Estado, entendiéndose también como el derecho de acceso a la información pública. Y viendo otra cara de la moneda, el concepto de transparencia en lo público, esta dimensión se concreta cuando es el Estado quien permite a la ciudadanía conocer el por qué, el cómo actúa y qué decisiones adopta, siendo por

ende la facultad que toda persona tiene para evaluar y fiscalizar directamente los servidores estatales, dentro de su rol de participación en la gestión pública.

Y conforme a ello, podemos observar que el acceso a la información pública apunta en el permiso de "mostrar" o de "permitir ver" por parte del Estado, mientras que la transparencia hace mención de una herramienta dotada a la ciudadanía, para alcanzar dicho objetivo, facultad que a su vez permite que las entidades del Estado divulguen de forma permanente información sin mediar requerimiento expreso y que además, estos mismos entreguen datos que sean efectivamente solicitados por cualquier persona; siempre que no corresponda información confidencial o reservada.

Es decir, nuestro ordenamiento jurídico ha tomado en base a la protección de datos personales, por un lado, el amparo de la intimidad y la autodeterminación informativa y por otra arista, el resguardo hacia la transparencia administrativa que favorece la probidad y que potencia la participación ciudadana. Sin embargo, dentro del marco de aplicación de la normativa encargada del régimen de acceso a la información pública, surge a la par otro punto débil y esto surge de la necesidad de definir qué tratamiento se le debe otorgar al Habeas Data personal en relación con el acceso a la información. Y, en efecto, nos encontramos ante dos bienes jurídicos de distinta naturaleza, es decir, la tutela de la información personal y el derecho de acceso, que constantemente al ser antagónicos, se manifiesta una gran tensión.

Por lo que, no solo el desarrollo de la legislación chilena bajo esta temática no ha ido a la par junto al avance de la tecnología actual, sino que además no ha habido claridad en cuanto a definir los diversos mecanismos y garantías que trae consigo el derecho a la protección de datos o del Habeas Data en general, provocando por ende que siempre estemos pasos atrás de la era cibernética, sobre todo en lo que respecta a la carga de la prueba, esto es, que la acción del Habeas Data al no englobar sanciones concretas y efectivas; y al emplear la misma metodología que cualquier acción judicial deducida ante los tribunales de justicia con defensa jurídica a coste del interesado, evidencia una desmotivación por parte de los titulares de dichos datos de ejercerlo, existiendo por ende una falta de propósito de su ejercicio dada la absoluta ausencia de la figura de autoridad de control, en cualquiera de sus formas.

En ese sentido, observamos que nuestro ordenamiento jurídico se ha quedado atrás en muchas normativas, dentro de las cuales deben necesariamente ir a la par con el desarrollo de la sociedad y adecuadas a la realidad virtual y tecnológica que estamos viviendo en nuestra rutina diaria. Una posible razón de ello se puede desprender que no toda la población tiene acercamiento o bien tiene una participación poco activa en el acceso a la tecnología de la información, entendiéndose este último a computadores, ordenadores, Banda ancha, entre otros; generando por consiguiente un impacto directo en el menoscabo de los derechos de nuestros usuarios.

Respecto a dichos puntos, es menester traer a colación un estudio realizado por la plataforma EMOL, encuesta realizada bajo la interrogante ¿En qué nivel se encuentra el país y qué falencias existen, respecto a la protección de datos personales en Chile? Al efecto, junto con el estudio realizado por el Observatorio de Sociedad Digital de la Universidad de Chile y la empresa CustomerTrigger (compañía que ayuda a mejorar las relaciones entre empresas y sus clientes),

al publicar el estudio "El Ciudadano y su Privacidad "frente a esta problemática, se ha registrado que la percepción de los chilenos frente a la protección de su privacidad y el traspaso de sus datos personales; concluye que *la gente per se no comprende el alcance que puede tener la filtración de los datos personales. No siente que sea un tema que le puede afectar. (…) El corazón del riesgo está en la confección, creación y manejo de las bases de datos"*[40].

Y, asimismo, respecto a la pregunta ¿Cómo es actualmente la seguridad y percepción de los chilenos frente al manejo de su información personal? Los resultados del estudio demostraron que "*la percepción de los chilenos sobre el uso y protección de sus datos personales, por parte de las organizaciones, es bastante negativa. De acuerdo con Maulén, el 92% de los encuestados señaló que el compartir su información personal con un tercero es un tema que les preocupa y, a su vez, el 93% manifestó sentirse "muy preocupado" de que las organizaciones usen sus datos para otros fines diferentes a los que fueron solicitados en su origen"*[41]. En efecto, la comunidad ha confesado que entrega sus datos personales sin mayor cuestionamiento y la normativa nada ayuda al parecer.

Es más, otra deficiencia que podemos deducir, enfocándonos en las dos dimensiones que hace referencia nuestra regulación consistente en la protección de datos personales, es decir, la tutela de la información personal de la persona y el ejercicio del acceso a la información pública; se traduce en que no podemos identificar en los diversos modelos normativos un equilibrio entre ambas dimensiones o bien cuál de ellas debe estar por sobre la otra, siendo nuevamente un problema a resolver producto de la no definición o claridad al respecto de cuál dimensión ha de aplicarse para obtener una garantía coherente y concisa del derecho en comento.

Esto viene dado a que, pese a que dentro de nuestro marco jurídico se hace referencia indistintamente a ambas tendencias, manteniéndose relacionadas entre sí, al no tener una fórmula absoluta y eficiente del tratamiento de los datos nominativos y el acceso a la información pública, nos generan estas dudas que se traducen al final "en un pasaje sin salida", sin obtener respuestas en nuestro propio ordenamiento. Como bien hace mención el autor Pablo Viollier:

> El principal problema de la Ley Nº19.628 es que no busca proteger a los individuos del tratamiento de sus datos realizado por terceros, sino regular el mercado de tratamiento de datos personales. Esto se traduce en: falta de sanciones efectivas a la vulneración de las normas, ausencia de regulación del flujo transfronterizo de los datos personales, uso de datos para marketing directo sin autorización del titular, falta de registro de bases de datos privadas, ausencia de una autoridad pública de control, excepciones amplias al consentimiento para el tratamiento de datos y falta de mecanismos procedimentales de resguardo efectivo[42].

[40] (Zecchetto, 2022)
[41] (Zecchetto, 2022)
[42] (Viollier, Pablo. 2017)

Y a la deficiencia anterior, se suma el hecho que la legislación no se ha adaptado a los estándares internacionales de la OCDE (Organización para la Cooperación y el Desarrollo Económicos), demostrándose una vez más la necesidad de adaptar la legislación nacional para repensar el cómo brindar a los usuarios el consentimiento previo para su uso de datos personales, el cual debe ser inequívoco, explícito, libre y sin ambigüedades, asimismo para establecer una limitación hacia las fuentes de libre acceso al público. Es de suma importancia que se introduzcan a nuestro marco jurídico los principios informantes de la OCDE, tales como la proporcionalidad, la calidad de los datos, especificación del propósito o finalidad del tratamiento de datos, limitaciones de uso, seguridad de los mismos, acceso y oposición de su titular, entre otros factores dentro de la misma gama.

Por ende, si bien como país estamos ante este espectacular y próspero avance dentro del marco del derecho, es condición necesaria para obtener al final una legislación centrada en la protección de los derechos de las personas, específicamente sobre sus datos personales, el dejar de lado los denominados "*intereses de lobby empresarial*" y que se proponga la protección verdadera del Habeas Data de los individuos desde una perspectiva de Derechos Humanos y no desde una arista de voluntad política.

Ahora bien, cuando hacemos mención del Ordenamiento Jurídico de Europa Occidental, como primeros puntos dota de una regulación, que a primeras luces brinda una protección hacia los datos de las personas jurídicas con el objeto de evitar una tramitación fraudulenta de los mismos y la comisión de delitos cibernéticos, siguiendo por ende la misma brecha del derecho a la intimidad reconocido en la Declaración Universal de Derechos Humanos (DDHH) de 1948, el cual es el asegurar a toda persona el derecho a la protección de la ley contra tales injerencias y ser un criterio para dimensionar la legitimación política de los sistemas democráticos, como dicho país tecnológicamente desarrollado. Asimismo, presenta una novedad junto con Estados Unidos de elaborar una normativa que procura brindar amparo a este nuevo bien jurídico, que es la "autodeterminación informativa o libertad informativa", donde en cuyo alero se les brinda a los titulares o usuarios un nutrido haz de facultades para así efectuar un control de la información mucho más acabado, con prescindencia de sí la misma alude o no a circunstancias de su vida privada.

En el mismo orden de ideas, Alemania se encuentra en plena armonía con el Convenio N.º 108, marco legal que vino a introducir un nivel de protección equivalente entre los Estados partes del mismo ante el denominado "*mosaico de diseños jurídicos de Europa",* obligando a los mismos a que dentro de sus ordenamientos incrusten principios generales y normas concretas, para prevenir finalmente la recolección y el tratamiento ilegal de datos personales, utilizados tanto por gobiernos como por el sector privado. A saber, dentro de las normas, ejemplificamos: 1)la calidad de los datos y lealtad en las operaciones de tratamiento sobre ellos, 2) protección especial hacia clases especiales de datos (datos sensibles) y prohibición de su tratamiento salvo excepción, 3) la adopción de medidas de seguridad física y lógica respecto de los datos; 4) el reconocimiento de los derechos de información, acceso, rectificación y cancelación, entre otros. Y respecto a los principios, hacemos mención del precepto de licitud y lealtad, el principio del

consentimiento informado del titular, la confidencialidad de los datos, etc. Es así como se plasma una legislación interna y uniforme, acorde a la concepción de la Unión Europea.

Siguiendo en la misma línea, dentro del ordenamiento jurídico alemán se introducen leyes que confieren una cierta autoridad de control nacional, que funciona a la par de una medida cautelar hacia el sistema de tratamiento de información, ya sea para conferir o denegar la autorización de dicho procesamiento de datos. Por ende, no solo se entabla dicho accionar por aquel titular de datos que estima que sus derechos y garantías se menoscaban por un tercero responsable de su tratamiento, sino que también se llega a extender a reclamaciones que este mismo usuario puede formular contra las decisiones de la autoridad de control y esto gracias a que se diseña un recurso jurisdiccional que tiene por finalidad garante el salvaguardar la autodeterminación informativa o mejor dicho la libertad informativa de las personas, cuando se vean amagados por el responsable del tratamiento ilícito y fraudulento de la misma información.

No obstante, dichos puntos positivos presentan inmediatas deficiencias. En primer lugar, si bien es cierto, Alemania ha diseñado una reglamentación para evitar el tráfico ilícito de datos y la comisión de delitos cibernéticos; y definiendo el derecho a la protección de datos personales dentro de la misma línea de amparo que la intimidad y vida privada, no prevé ningún elemento o factor que reconozca de forma inmediata la autodeterminación informática de forma explícita, existiendo por consiguiente un déficit en el amparo hacia el cuidado de los datos personales de las personas naturales y desarrollo a cabalidad de la misma garantía como bien jurídico "novedoso y autónomo". Y aquello es inevitable, puesto que estamos frente a un desafío inesperado e impredecible, que es el enfrentar la realidad virtual que convive con nosotros día a día y el diseñar un cuadro jurídico para avanzar junto a ella al mismo nivel y desenvolvernos de la misma manera, que claramente implica un trabajo desafiante y que amerita mayor pulcritud y aterrizaje.

Otra deficiencia se manifiesta en que, al ser los datos o el derecho a la protección de los mismos un bien jurídico relativamente nuevo, para Europa en sí ha evidenciado una difícil tarea en cuanto a determinar cuál es su alcance, extensión y ponderación dentro del interés común de la sociedad, precisamente por haber logrado solamente consensos mínimos sobre su base y aproximación normativa, evidenciándose una vez más la necesidad de un reconocimiento y promoción de mecanismos de autocontrol generales, puesto que los datos son una herramienta valiosa que nos permite predecir no solo el cómo es una persona en sí de forma aislada, sino que además orienta y perfila a toda una comunidad, lo cual significa una gran tentación para industrias, empresas e inclusive para partidos políticos.

Es más, dado que el derecho a la protección de datos está definido en la legislación de la UE, al no aplicarse dichos preceptos a aquellas personas físicas que no se encuentren dentro de la misma, genera un problema en brindar una seguridad adecuada en dicha materia, puesto que el certificar tecnologías para proteger la intimidad, su independencia como usuarios, que los mecanismos de control (vale decir: de difusión, publicidad, asistencia, fiscalización y de sanción) le sean representativos en sus derechos y garantías; y que tengan acceso a una legislación fundada y oportuna es casi inexistente, sobre todo en temas y riesgos constantes de los denominados "ciberataques", que cada día van tomando mayor amplitud tanto en escala

europea como internacional, donde la rapidez de la obtención de datos y la capacidad de almacenamiento se transforman en pesadillas del tercer mundo. Y respecto a este último punto, como precisa Alejandra Castillo Ara:

> En materia de cibercrimen, una de las grandes dificultades que representan los delitos cibernéticos al momento de la obtención de su detección y persecución es el problema de la territorialidad. El derecho penal es por excelencia un área de regulación local. Este paradigma de funcionamiento del derecho penal ha sido desafiado precisamente por los avances de la tecnología cibernética y, por tanto, por los modos de ejecución que revisten los delitos cibernéticos (...) La lógica indica que, en materia de delitos cibernéticos, la territorialidad como principio debería desaparecer y la cibercriminalidad deberían operar bajo el principio de jurisdicción universal como ocurre con crímenes de lesa humanidad, en el entendido de que ambos tienen como objeto de protección, bienes o intereses que son centrales para la conservación del Estado como organismos político y social[43].

[43] (Castillo, Alejandra. 2020)

CONCLUSIONES

A lo largo del presente trabajo, hemos podido evidenciar la escasez de investigación y la poca definición de esta garantía jurídica que nos deja la nueva realidad virtual, es decir, el derecho a la protección de datos personales, cuyo bien jurídico es la autodeterminación informativa y el Habeas Data, pese a la imposición y relevancia que ha tenido esta nueva ciencia legal en nuestro presente. Empero, tanto Chile como Alemania si bien han relacionado el derecho en comento bajo el alero de la privacidad, dignidad, honra e intimidad, su poco desarrollo y alcance que ambos ordenamientos le han entregado, demuestra la complejidad de que florezca y se inserte esta nueva garantía en términos específicos en nuestra sociedad.

El derecho a la protección de datos personales ha obtenido protagonismo ante el hecho que, el ser humano del siglo XXI día a día va dejando una estela de datos que se encuentran dispersos en distintas plataformas, ya sean redes sociales, plataformas de Banco, cuentas de Google y en los diversos medios de Internet; por lo que actualmente, con la utilización de nuevos medios tecnológicos y su posibilidad de agrupar y tratar de interpretar dichos datos para crear un perfil determinado del individuo, pueden ser objeto de manipulaciones. Por ende, su desarrollo en sede normativa y la recopilación de las experiencias y puntos de vista de otros países, más aún teniendo presente la rapidez del desarrollo de la tecnología, ha sido una preocupación palpable. Es más, el marcado desarrollo tecnológico, demuestra el menester de llevar el reconocimiento del derecho a la autodeterminación informática en sede constitucional y alcanzar su carácter fundamental.

Es más, el próspero avance del Habeas Data desde una perspectiva internacional ha sido asimétrico, pese la necesidad de generar estándares comunes para evitar los riesgos que supone el desarrollo desenfrenado de la tecnología dentro de un mundo globalizado, como por ejemplo los principios sobre la privacidad y la protección de Datos Personales de la Organización de los Estados Americanos (OEA), donde su departamento de derecho internacional sobre asuntos Jurídicos brinda 13 principios que reflejan las distintas aproximaciones que prevalecen en los estados miembros, sobre los temas centrales de la protección de los datos personales, dentro de los cuales encontramos el consentimiento, las finalidades, medios para la captación y tratamiento de estos datos, el flujo transfronterizo, entre otros; pero hablamos aquí netamente a nivel de OEA y actores que intervinieron en dicho proceso como el Comité Internacional de la Cruz Roja, la Comisión Interamericana de Mujeres y la Red Iberoamericana de Protección de Datos, más no genera una aplicación para otros sectores del mundo, produciéndose por consiguiente esta asimetría.

Y si bien el desarrollo de este derecho tiene estrecha relación con el derecho a la vida privada, su desenvolvimiento en forma explícita ha sido lento, puesto que sus avances y generación han provocado de forma inmediata críticas en cuanto a su delimitación y su relación con otros derechos o garantías en contextos específicos, permitiéndonos afirmar que la falta de experiencia e investigación por parte de la doctrina y jurisprudencia, ya no es un argumento viable en la actualidad. El derecho a preservar el control sobre nuestros datos personales y la aplicación de las nuevas tecnologías de la información, deben ser el contexto en el cual el legislador puede consagrar este derecho fundamental de carácter personal.

Por lo que, nuevamente, reflejamos la necesidad de diseñar estándares comunes que permitan proteger de manera efectiva a las personas, pero con una aproximación universal, no solo para Europa, Asia, Oceanía o dentro de América, sino que ya hablando a nivel internacional, para que con ello se pueda garantizar el mayor disfrute de los derechos y libertades de las personas dentro de este término, así como para que esta innovación contribuya en el desarrollo socioeconómico en esta nueva era digital y lograr una sociedad interconectada como la actual.

Asimismo, como analizamos en el marco de nuestra investigación, el vertiginoso desarrollo del mundo cibernético ha permitido que distintas organizaciones o diversas plataformas utilicen cada vez más técnicas como la inteligencia artificial (IA), a fin de hacer más eficientes los procesos y la toma de decisiones, incluso concretando a esta herramienta en una oportunidad para el procesamiento de información, por ejemplo, relativa a estados de salud, preferencias comerciales, o simplemente para buscar información en el ciberespacio, gracias al análisis masivo y sistemático de la pesquisa, que incluye casi siempre, datos personales que identifican o hacen identificables a los humanos. Y derivado de lo anterior, existe una constante preocupación respecto del uso masivo de esta clase de facilidades que brinda la IA, como por ejemplo tratamientos indebidos de datos (falta de cumplimiento normativo o de incorporación de límites éticos) o falta de medidas de seguridad o errores en el diseño de la técnica, donde ambas prácticas se traducen en una violación hacia los derechos humanos desde una perspectiva del derecho a la vida privada hasta el derecho a la intimidad y a la protección de datos personales.

Y como mencionamos en puntos anteriores, cuando estamos ante tratamientos de información que contienen datos personales a través de sistemas de inteligencia artificial, si bien existen marcos normativos de índole local y en algunos casos se han llegado a consensos sobre principios y aplicación de ciertos preceptos jurídicos a nivel regional o internacional en materia de protección de datos personales, aun así no ha sido suficiente para alcanzar un debido amparo global para dicha garantía, donde no todo se traduzca en mecanismos normativos, sino que una mezcla con mecanismos que permitan el efectivo ejercicio y garantía de los derechos humanos por parte de los actores involucrados en la IA y que exista una aplicación de ello a nivel internacional, no constituyendo la limitación territorial una piedra en el camino para tan anhelada meta. Es decir, resulta pertinente en el marco del Habeas Data conseguir un correcto balance entre la innovación y dignidad de la persona.

Cabalmente, la novedad de este derecho y su poco conocimiento, genera tanto para los titulares de datos personales como para la jurisprudencia, dudas acerca de la especificidad y exactitud de este bien jurídico y cuál debe ser la protección que amerita. Al efecto, respecto a la comparación de ambos países, en primer término, creemos que precisamente dicho desconocimiento se debe a la poca recepción por parte de Chile de la doctrina internacional y la poca iniciativa por parte de nuestro país de desplegar una investigación mucho más explícita sobre la materia en comento, es decir, esta ignorancia se debe a la poca claridad a nivel legal y constitucional. Y en segundo término, en lo que respecta a Europa Occidental, Alemania, la irrisoria aplicación de este derecho debe su motivo al inamovible enfoque tiene, netamente a nivel empresarial y su combate contra la cibercriminalidad en torno a los datos personales de

parte de los organismos del Estado y subordinados, más no se evidencia como país una regulación específica y autónoma del derecho a la protección de datos personales para personas naturales y jurídicas; y su interacción con los demás organismos estatales.

En nuestro país, la protección de datos personales parece ser un reto que aún en el presente se mantiene en una gran incógnita, pues se han realizado esfuerzos para priorizar su tratamiento y trámite en nuestro Congreso Nacional, pero sin resultados efectivos. Esto dado que, al ser un país con una cultura correctiva y no preventiva, sumando el hecho que estamos acostumbrados a que todo debe estar redactado en una ley para que nuestra conducta se adecue a ello al pie de la letra, la falta de un marco normativo que esté a la altura del debido resguardo, para que de esta forma se proteja de forma correcta y eficaz el derecho de la protección hacia los datos personales, mantiene aún este desafío en la actualidad, quedándonos atrás en los avances de la tecnología.

Por tanto, creemos que es fundamental, dentro de una primera arista, la extensión del artículo 19 Nº4 de nuestra Constitución Política de la República que haga mención expresa y de forma indubitada de este derecho a la autodeterminación informativa y del Habeas Data para personas naturales y jurídicas; y que claramente tiene relación con la privacidad, el honor y la intimidad. Y, por otra arista, estimamos pertinente que el proyecto de esta nueva ley que regula la Protección y el Tratamiento de los Datos Personales y crea la Agencia de Protección de Datos Personales, contenga en su espíritu una real protección a sus titulares, que mencione con expresa claridad los derechos y deberes tanto de los usuarios como de los organismos que tratan con dichos datos, que limite la transmisión de datos a terceros; que prohíba la transmisión por cualquier vía sin permiso de su titular, que entable una lista taxativa de las fuentes o informaciones accesibles a todo el umbral público, entre otros aspectos del mismo lineamiento.

Finalmente, en lo que respecta a Alemania, creemos que el país de Europa Occidental no debería limitar la aplicación del Reglamento General de Protección de Datos (RGPD) de la Unión Europea del año 2018[44]; y reforzar única y exclusivamente las directrices del campo de amparo de datos para empresas y autoridades en el empleo de los llamados datos personales, sino que sea uno de los principales instrumentos para combatir la cibercriminalidad ante el tratamiento indebido de los mismos que manejen empresas, entes del Estado y personas naturales, ideándose por ende un marco normativo o mejor principios y preceptos generales, de carácter uniforme, para todos los estados federados de Alemania e incluso aplicable a toda Europa, para todos los usuarios del mundo digital; y que precisamente regule la autorización que estos le brinden a la diversidad de organismos, amparando coherentemente el Habeas Data, para que haga frente a la realidad virtual que convive con nosotros día a día y no sea el elemento de la territorialidad el principio que provoque su desplome y vulneración, terminando de una vez por todas este gran dilema de proteger los datos personales y el eventual beneficio del tratamiento de los mismos, interrogante aún palpable en pleno siglo XXI.

[44] Reglamento General de Protección de Datos (RGPD): Reglamento que tiene por objeto el refuerzo de las directrices sobre el cómo las empresas y las autoridades pueden usar datos personales

BIBLIOGRAFÍA

- Bär, D., & Artigas, C. (2021). *Joint Declaration on cooperation and exchange of best practices in the field of self-sovereign identity between the Federal Republic of Germany and the Kingdom of Spain*. Recuperado de https://www.bundesregierung.de/resource/blob/997532/1947314/4dc5ac1821962d969304886d9c09b768/2021-07-29-joint-declaration-on-cooperation-spain-germany-data.pdf.

- Benda, Ernst, 2001. *Dignidad humana y derechos de la personalidad*. En Manual de Derecho Constitucional, 2da edición. Madrid: Marcial Pons, Ediciones Jurídicas y Sociales, págs. 242 y 243. ISBN 97884724885.

- Bertelsen, R; Corral, H., González, F.; Jara, R., Jijena, R., Mendoza, R., y Vial, F., 2001. Tratamiento de Datos Personales y Protección de la Vida Privada: *Estudios Sobre la Ley Nº19.628 Sobre Protección de Datos De Carácter Personal* [en línea]. S.L: Universidad de los Andes, Facultad de Derecho. [Consulta: 23 Octubre 2022] ISBN 956-7160-21X. Disponible en: HTTPS://WWW.UANDES.CL/WP-CONTENT/UPLOADS/2019/03/CUADERNO-DE-EXTENSIÓN-JUR%C3%ADDICA-N°-5-TRATAMIENTO-DE-DATOS-PERSONALES-Y-PROTECCIÓN-DE-LA-VIDA-PRIVADA.PDF

- Castillo, A. 2020. "*Desafíos de la Protección de Datos Personales en el Derecho de la Unión Europea"* Actualidad Jurídica [en línea] Disponible en: HTTPS://DERECHO.UDD.CL/ACTUALIDAD-JURIDICA/FILES/2021/01/AJ42-P27.PDF

- Cerda, A. 2003. *Autodeterminación informativa y leyes sobre Protección de Datos.* Revista Chilena de Derecho Informático, Vol. 3. Disponible en: HTTPS://DERECHOINFORMATICO.UCHILE.CL/INDEX.PHP/RCHDI/ARTICLE/VIEW/10661

- Congreso Nacional de la República de Chile. (2005) Decreto Nº100. Fija el texto refundido, coordinado y sistematizado de la Constitución Política de la República de Chile. Promulgado: 17 de Septiembre de 2005. D.O: 22 de Septiembre de 2005. In Decreto (VOL. 100) HTTPS://WWW.BCN.CL/LEYCHILE/NAVEGAR?IDNORMA=242302

- Contreras, P. 2020. *El Derecho a la Protección de Datos Personales y el Reconocimiento de la Autodeterminación Informativa en la Constitución Chilena.* Estudios Constitucionales [en línea], VOL 18 Nº2, pág. 120. [Consulta: 23 Octubre 2022] ISSN. ISSN 0718-0195. DOI 10.4067/S0718-52002020000200087. DISPONIBLE EN: HTTP://WWW.ESTUDIOSCONSTITUCIONALES.CL/INDEX.PHP/ECONSTITUCIONALES/ARTICLE/VIEW/693

- (Diccionario Panhispánico del Español Jurídico [sitio web], 2022. Derecho de Protección de Datos Personales [Consulta: 04 marzo 2023]. Disponible en: https://dpej.rae.es/lema/derecho-de-protección-de-datos-personales)

- Grundgesetz für die Bundesrepublik Deutschland. (1949) https://www.gesetze-im-internet.de/gg/BJNR000010949.html Traducción en Español Disponible en: https://www.bundestag.de/resource/blob/658022/160ce346b7f4d14f05fcbf8080a60fc0/flyer_ley_fundamental_pdf-data.pdf

- Gacitúa, A. 2014. *El Derecho Fundamental a la Protección de Datos Personales en el Ámbito de la Prevención y Represión Penal Europea (En Busca del Equilibrio entre la Libertad y la Seguridad)* [en línea] Tesis para optar al Grado de Doctor En Derecho Público del Programa: "Las Transformaciones del Estado de Derecho Desde la Perspectiva de la Filosofía del Derecho, El Derecho Constitucional y el Derecho Penal". Santiago de Chile: Universidad Autónoma de Barcelona. [Consulta: 22 Octubre 2022] Disponible en: https://ddd.uab.cat/pub/tesis/2014/hdl_10803_284352/alge1de1.pdf

- Labbé, S y Latrille P. 2018. *Protección de los Datos Personales en Chile, su Tratamiento y Comercialización. Análisis y Críticas a la Ley Nº19.628.* [en línea] Memoria Presentada a la Facultad de Derecho de la Universidad Finis Terrae Para Optar al Título de Licenciado En Ciencias Jurídicas y Sociales. [Consulta: 8 Noviembre 2022] Disponible en: https://repositorio.uft.cl/xmlui/bitstream/handle/20.500.12254/1494/labbe-latrille%202018.pdf?sequence=1

- Lazpita Gurtubay, M. *"Análisis comparado de las Legislaciones sobre Protección de Datos de los Estados Miembros de la Comunidad Europea"* [en línea]. Tesis doctoral. Barcelona: Universidad Autónoma de Barcelona [consulta: 15 de abril] Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=248383

- Ministerio Secretaría General de la Presidencia. Ley Nº19.628. Sobre Protección de la Vida Privada. Promulgada: 18 de Agosto de 1999. D.O: 28 de Agosto de 1999 [en línea]. Santiago: S.N. [Consulta: 22 de Octubre 2022] Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=141599

- Navarro Beltrán, E. 2011, *Recopilación de jurisprudencia del Tribunal Constitucional*, Primera Edición, Santiago de Chile, Editorial producciones gráficas Ltd.

- Pérez, L, 2017. *"Seguridad versus Intimidad y Cuidadanía; Papel del Delegado de Protección de Datos y Responsabilidad de las Instituciones y Empresas en el nuevo Reglamento Europeo de Protección de Datos, Torino* [en línea]. Disponible en: https://accedacris.ulpgc.es/bitstream/10553/106740/2/seguridad_versus_intimidad.pdf

- Pontificia Universidad Católica [sitio web], 2023. Tratamiento y Protección de Datos UC. En: *Uc.cl* [en línea]. Disponible en: https://protecciondedatos.uc.cl/politica/dp [Consulta: 4 de marzo 2023]

- Quezada, F. (2012): "La protección de datos personales en la jurisprudencia del Tribunal Constitucional de Chile". *Revista Chilena de Derecho y Tecnología* (Vol. 1. No. 1).
- Salvador, B, 2019. Funas en redes sociales vs protección de datos personales. En: *Estadodiario* [Disponible en: https://estadodiario.com/columnas/funas-en-redes-sociales-vs-proteccion-de-datos-personales/ [Consulta: 12 de enero 2019]

- Satzger, Helmut. "*La protección de datos y sistemas informáticos en el derecho penal alemán europeo. Tentativa de una comparación con la situación legal en Colombia*"

- Viollier, Pablo. 2017. "El Estado de la protección de Datos Personales en Chile" *Derechos Digitales América Latina* [en línea] [Consulta: 23 de abril 2023] Disponible en: https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf

- Zecchetto Rocco, Marco, 2022. Estudio aborda la protección de datos personales en Chile: ¿En qué nivel se encuentra el país y qué falencias existen? *Emol Social Facts.* 5 de diciembre.

NORMAS CITADAS

- Alemania, Grundgesetz für die Bundesrepublik Deutschalnd, 1949, HTTPS://WWW.GESETZE-IM-INTERNET.DE/GG/BJNR000010949.HTML Traducción en español disponible en: HTTPS://WWW.BUNDESTAG.DE/RESOURCE/BLOB/658022/160CE346B7F4D14F05FCBF8080A60FC0/FLYER_LEY_FUNDAMENTAL_PDF-DATA.PDF , artículos 1, 2, 10.1 y 13.

- Chile, Constitución Política de la República de Chile, texto actualizado en Decreto Nº100, Segpres: fija el texto refundido, coordinado y sistematizado de la Constitución Política de la República de Chile, D.O 22-septiembre-2005, artículo 19 Nº4)

- (Council of Europe), *Convenio Europeo de Derechos Humanos* (CEDH), 67075 Strasbourg cedex, Francia, publicada por el Tribunal Europeo de Derechos Humanos, 1950, modificada en 2021.

- (Ministerio Secretaría General de la Presidencia). Ley Nº19.628. Sobre Protección de la Vida Privada. Promulgada: 18 de Agosto de 1999. D.O: 28 de Agosto de 1999 [en línea]. Santiago: S.N. [Consulta: 22 de Octubre 2022] Disponible en: HTTPS://WWW.BCN.CL/LEYCHILE/NAVEGAR?IDNORMA=141599

- (Ministerio de justicia, 2023, Código Civil, Editorial jurídica, Vigésima novena Edición; Santiago de Chile, pp.390)

- (Organización de los Estados Americanos) (OEA), Departamento de Derecho Internacional, Secretaría de Asuntos Jurídicos, *Principios Actualizados sobre la Privacidad y la Protección de Datos Personales,* Capítulo XIV, OEA/Ser.D/XIX.20, ISBN 978-0-8270-7414-9, 2022.

- (Unión Europea (UE)), *Reglamento General de Protección de Datos (RGPD),* 2016/679, publicada en DOUE, 2018.