FACULTAD DE DERECHO
UNIVERSIDAD DE CHILE

Tesis para optar al grado de
licenciado en ciencias
jurídicas y sociales

Big Data y su aplicación a las decisiones judiciales automatizadas

Autora: Fernanda Carvajal Gezan

Profesora Guía: Lorena Donoso Abarca

Julio 2022

Contenido

AGRADECIMIENTOS

Para Dusan Gezan.
Abuelo, amigo y compañero.

Gracias por compartir conmigo la curiosidad por el mundo y las ansias de aprenderlo todo; por las conversaciones infinitas, la música, la cocina y los libros; por tu apertura a los cambios, por esa capacidad crítica y nuestros miles de imaginarios; por hacer tu parte en la construcción de un mundo más justo, por correr los riesgos y poner tesón y pasión en todo lo que hiciste; por creer en mí y apoyarme en todos mis proyectos y por acompañarme en cada etapa de mi vida, aun después de tus días…

"Los músicos no se retiran, se detienen cuando no hay más música en ellos"
Luis Armstrong

INTRODUCCIÓN

Para nadie resulta novedoso decir en la actualidad que vivimos una época de grandes cambios en que día a día podemos sorprendernos por algún salto en materias de ciencia y tecnología. Desde la construcción de casas y creación de órganos por medio de impresoras 3D, los ensayos de Space X en su avanzada por llevar a la humanidad a Marte, el apabullante desarrollo de la industria automotriz que busca disminuir las emisiones de carbono y podría lograr sistemas seguros de conducción automatizada en ciudades, los conciertos virtuales y el proyecto del Metaverso, entre tantas otras innovaciones que hasta hace poco sólo se podían imaginar en productos de ciencia ficción.

Naturalmente, entre las muchas esferas de aplicación para estas nuevas tecnologías, el universo jurídico no podía quedar fuera, por lo que hemos podido conocer durante los últimos años una serie de plataformas que asisten a los abogados en el registro y actualización de sus causas, que les informan la etapa judicial en que se hallan, informan requisitos, plazos e identifican sitios y materias de interés que resulten afines a sus funciones. Asimismo, la tramitación judicial en Chile se lleva a cabo de manera preponderantemente electrónica desde el año 2016, estando digitalizados los expedientes y documentos y facilitándose una oficina judicial virtual para cada jurista, desde la cual pueden realizar todos los trámites necesarios.

Pero las iniciativas en nuestro campo profesional no se reducen a la mera digitalización de procesos, sino que, ya en la actualidad, se han incorporado mecanismos provistos de inteligencia artificial que facilitan la toma de decisiones judiciales, cuyas funciones pueden consistir en el análisis de jurisprudencia asociada, en la ponderación de los antecedentes, análisis predictivo de comportamiento, en la propuesta de textos para el fallo de causas, al punto que en Estonia evalúan la posibilidad de implementar jueces robot para la decisión de causas de baja cuantía. Todo esto tiene como correlato el objetivo de disminuir los trámites burocráticos, homologar criterios de evaluación, tener a la vista una cantidad superior de información a la hora de tomar decisiones y acelerar sustancialmente los tiempos habituales de la administración de justicia.

No obstante aquello, las significativas mejoras que puede traer consigo el progreso tecnológico, tienen su contracara en la subsecuente multiplicidad de hipótesis abusivas que cada

uno de estos proyectos puede acarrear cuando no existe una regulación adecuada que limite sus ámbitos y/o fines de aplicación.

Como se verá en este trabajo, una utilización mal intencionada de herramientas de procesamiento masivo de datos puede tener consecuencias sumamente gravosas tanto para las personas como para las sociedades en su conjunto. Es por esta razón que se ha planteado la necesidad de poner los énfasis en su adecuada regulación y en las actividades de fiscalización y, en caso de detectarse contravenciones al ordenamiento normativo, la aplicación de la sanción correspondiente. Ello es más evidente si consideramos la masificación en el uso de sistemas de procesamiento masivo de datos y el creciente interés por sus aplicaciones, lo que ha alcanzado al derecho procesal. El desafío es lograr una utilización adecuada de estas tecnologías, que sea respetuosa de los derechos de las personas y que cumpla un rol de provecho para las sociedades.

Este trabajo busca analizar las implicancias de la aplicación del big data e inteligencia artificial en la resolución de conflictos de relevancia jurídica.

En nuestro análisis pondremos en contexto diversos aportes y riesgos derivados de los sistemas de tratamiento masivo de información a partir de experiencias relevantes en el mundo que permitan visibilizar sus complejidades. Luego, abordaremos la regulación que se ha dado al Big Data en la Unión Europea y, posteriormente en nuestro país, ambos desde perspectivas civiles, administrativas y penales, tomando en consideración Tratados Internacionales y proyectos de ley en tramitación, con lo que se espera evidenciar el carácter multidimensional del fenómeno en comento y conocer sus objetivos y limitaciones. A propósito de lo anterior, se analizarán de manera pormenorizada los nuevos derechos incorporados en las legislaciones más modernas al efecto, poniendo especial atención al derecho de impugnación, sus características y necesidades procesales especiales.

Teniendo a la vista este sistema de reglas, la investigación expondrá el caso de Estonia, país pionero en la ciencia de datos que se ha empeñado en tecnologizar todos los aspectos posibles de su administración pública, convirtiéndose en el país más digitalizado del mundo según la Revista Forbes.

Teniendo a la vista un país con tales características y distancia en su desarrollo tecnológico, será posible hacer una bajada más concreta a los aspectos que es necesario considerar al momento de implementar mecanismos de procesamiento masivo de datos e

inteligencia artificial en algunas actividades de la administración del Estado, en particular considerando su referida iniciativa de incorporar jueces robot para la resolución de controversias de baja cuantía, lo que nos aproximará a la respuesta de una de las principales interrogantes planteadas en el trabajo, a saber, si es que, partiendo del esquema normativo actual, es factible la implementación de sistemas de toma de decisiones automatizadas en sede judicial. Una afectación significativa del ámbito procesal tal como lo conocemos y un asunto importante de analizar en relación con la aplicación de algunos principios del derecho, como la igualdad ante la ley, la presunción de inocencia, la aplicación de un justo y racional procedimiento establecido de antemano y conocido por las partes y la obligatoriedad de justificar una sentencia, entre otros.

Así, se pondrá en contexto la eventual iniciativa de introducir programas de tratamiento automatizado de datos en la actividad jurisdiccional chilena, reflexionando, por un lado, acerca de sus posibles usos y beneficios y, por otro, evidenciando sus potenciales consecuencias y las medidas a adoptar para conciliar su utilización con las bases del debido proceso a fin de proponer un margen de uso razonable dado el estado de avance tanto de las tecnologías a aplicar, como de la normativa que regiría su utilización.

Como es sabido, una iniciativa de tales características constituye un enorme desafío para el derecho, pero sobre todo para su aplicación, toda vez que en el papel es sencillo imaginar opciones e idear un sistema coherente. Sin embargo, la tecnología avanza de manera disímil, se aplica de maneras diversas y siempre se encarga de abrir caminos que no suelen preverse por el legislador, sin mencionar la apabullante diferencia en la velocidad con que aparecen nuevas tecnologías llenas de posibilidades y efectos y la capacidad que tiene la ley para idearse, discutirse y materializarse como respuesta a un evento.

Es en consideración a este dilema que el cuarto y último capítulo se referirá en términos amplios a los desafíos regulatorios que enfrentamos en la actualidad respecto de los avances en sistemas de procesamiento masivo de datos aplicados a toda índole de materias, que no han sido previstos total o parcialmente por las leyes vigentes o en tramitación y que, por tanto, requieren de una interpretación flexible de las normas para dar respuesta a sus implicancias protegiendo a los ciudadanos, las sociedades y sus instituciones.

Los desafíos regulatorios referidos en este capítulo no necesariamente hacen referencia al tratamiento de datos personales, sino de datos en general, pero es relevante destacarlos en vista

de que, dada su forma de aplicación, pueden derivar en la afectación de derechos más allá de la privacidad, lo que constituye un riesgo para las personas y muchas veces para la sana convivencia social, circunstancia que los constituye en fenómenos que no pueden ser ignorados y a los que se debe dar una pronta respuesta por parte del legislador. Es por ello que en este ámbito el trabajo ofrece una panorámica sobre el fenómeno del tratamiento masivo de datos, sus usos beneficiosos y perjudiciales, sus áreas actuales y potenciales de aplicación, la evolución de la normativa desarrollada al efecto, las normas actuales en sede civil, administrativa y penal, tanto europeas como chilenas, la exposición del contexto estonio respecto de la utilización de programas con inteligencia artificial para resolver asuntos de la administración pública y la pregunta central acerca de si, partiendo de esta experiencia, sería viable implementar en Chile mecanismos de procesamiento masivo de datos en el marco de los procedimientos judiciales, analizando bajo qué supuestos, con qué tipo de precauciones y en qué medida estos podrían constituir un aporte para nuestras judicaturas.

CAPÍTULO I: El Big Data. Comprensión del Fenómeno

1.- El Big Data y sus usos:

Hacia octubre de 2018, Brasil se preparaba para la segunda vuelta de su elección presidencial entre los candidatos Jair Bolsonaro y Fernando Haddad, quienes, respectivamente, habían obtenido un 46% y 29% de las preferencias en primera vuelta. En este contexto, el Tribunal Superior Electoral (TSE) anunciaba el lanzamiento de un sitio web destinado a desacreditar las publicaciones en redes sociales que cuestionaran la legitimidad de los comicios. Adicionalmente, la presidenta del TSE, Rosa Weber, se reunía con representantes de ambos candidatos, además de representantes de Google, Facebook y la prensa, a fin de abordar la inédita cantidad de noticias falsas o *fake news* que inundaron las redes sociales y de mensajería, como Facebook y WhatsApp, durante el período de campaña y que perjudicaban mayoritariamente al candidato Fernando Haddad. Para entonces, 31 de los 35 partidos políticos del país habían suscrito un compromiso con el TSE en orden a no difundir noticias falsas (América Economía, 2018).

Dada la preocupación suscitada por la cantidad de información falsa circulante y la consecuente confusión de la opinión pública, la Fiscalía abrió una investigación para determinar si habría empresas de tecnologías de la información diseminando de manera estructurada noticias falsas referentes a los candidatos. En paralelo, WhatsApp intentaba detectar comportamientos sospechosos en las cuentas de los usuarios y desactivar aquellas que le parecía necesario. Al 20 de octubre se habían bloqueado cientos de miles de cuentas, entre las cuales estaba la de Flavio Bolsonaro, hijo del candidato, a quien se le atribuyó este tipo de actividad. Adicionalmente la empresa anunció medidas legales para impedir el envío de mensajes masivos y *spam* a través de la plataforma, a números telefónicos sin contar con la autorización de sus titulares (BBC, 2018). No conforme con ello, Facebook instaló una oficina, *"the war room"*, dedicada exclusivamente a desactivar fuentes de desinformación y discursos de odio. Para ello elaboraron etiquetas que advertían sobre la falsedad de algunas cuentas y prevenían sobre los *spam*, prohibieron los contenidos falsos y llegaron a bajar historias de la red previa orden judicial (Levin, 2018).

Aunque la investigación relativa al direccionamiento estructurado y/o automatizado de noticias falsas durante las campañas presidenciales no ha sido concluyente, a un año de la victoria electoral de Jair Bolsonaro, el Gerente de Políticas Públicas y responsable de elecciones, programas y campañas políticas de WhatsApp, Ben Supple, en su participación en el Festival Gabo en Colombia, se refirió a la amenaza que representaba el que, durante dichas elecciones, hubiera empresas que mandaban grandes

cantidades de mensajes con contenidos no comprobables, para llegar a una mayor cantidad de personas. Además, Supple se refirió al grado de vulnerabilidad que caracteriza a grandes segmentos de la población brasileña a la hora de recibir contenidos falsos, dado que no tienen acceso a fuentes de información de calidad ni a espacios de verificación de contenidos, por lo que dependen desproporcionadamente de WhatsApp para informarse (Gabo, 2019).

En otro contexto, recordemos el polémico rol de la compañía Cambridge Analytica en las elecciones presidenciales de EE.UU. y el plebiscito del Brexit en Inglaterra el año 2016. En ambos casos esta empresa fue contratada para recopilar información de los gustos, intereses, opiniones y miedos, entre otros criterios, de los votantes que eran usuarios de Facebook y que accedían desde sus cuentas a un *test* de personalidad de la empresa Global Science Research que permitía también conocer los contactos de la persona que contestaban dicha evaluación. Esto permitió elaborar perfiles que luego fueron utilizados por *Cambridge Analytics* para ofrecer servicios de *microtargeting* conductual y apoyo a campañas políticas, facilitando el envío de propaganda personalizada y sesgada en base a sus propias personalidades, temores, móviles y preferencias (Dance, 2018).

El año 2013 un grupo de investigadores de la Universidad de Cambridge publicó un estudio que daba cuenta de la facilidad y alto grado de precisión con que pueden atribuirse determinadas características personales sensibles a los usuarios de Facebook basándose únicamente en sus *"likes"*. Entre los atributos que pueden deducirse están la orientación sexual, origen étnico, posición política y religiosa, rasgos de personalidad, inteligencia, felicidad, uso de sustancias adictivas, separación parental, edad y género. El estudio realizado sobre 58.000 voluntarios arrojó un grado de acierto de 88% respecto de la orientación sexual, 95% en la distinción entre afroamericanos y caucásicos y 85% respecto de su preferencia política entre Demócratas y Republicanos, entre otros aspectos (Michal Kosinski, 2013).

Entre las metodologías utilizadas para manipular el voto, la utilizada en Brasil consistió en la difusión de noticias falsas que generalmente promueven el miedo y el odio, a través de las redes aprovechándose de la ignorancia y los prejuicios de la población a la que se apunta, puesto que los usuarios tienden a hacer eco de estas (des)informaciones de manera precipitada y sin mediar comprobación alguna.

Para maximizar los resultados, han sido ampliamente utilizados los denominados "*bots*", esto es, sistemas informáticos programados para realizar tareas repetitivas que imitan el comportamiento humano, tales como compartir sostenidamente publicaciones de redes sociales. Al respecto, un estudio de la Universidad de California del Sur, para el año 2017, sostiene que entre un 9% y un 15% de las cuentas anglohablantes activas de Twitter correspondían a *bots* (Onur Varol, 2017). En todo caso,

además de su uso para la difusión de noticias falsas, los *bots* se usan profusamente con finalidades legítimas.

Si bien se trata de un método desestructurado, la preocupación se deriva de que las *fake news* se difunden a una velocidad muy superior a las informaciones verídicas, e incluso aquellas de carácter rectificatorio, pues suelen estructurarse en términos que causan una fuerte impresión en el lector, refiriéndose a sucesos acaecidos graves o impactantes, o alertas de riesgos que demandan acciones de prevención urgentes. Por ello, aunque los *bots* realicen una difusión equivalente tanto del contenido falso como del rectificatorio, las personas son más propensas a compartir los contenidos falsos (Soroush Vosoughi, 2018).

Otra metodología aplicada a la manipulación electoral utiliza procesamiento masivo de datos personales en los términos señalados respecto del caso Cambridge Analytics. En este caso en base a los perfiles se realizan predicciones sobre las emociones y comportamiento de las personas, para luego diseñar y direccionar mensajes estructurados de manera coherente con el perfil, incluyendo determinados aspectos de campaña, noticias, entrevistas, debates y, en ocasiones también, noticias falsas que tengan el potencial de inclinar la intención de voto en favor del emisor; en muchas ocasiones, el receptor ni siquiera tiene conocimiento de estar siendo bombardeado con propaganda política durante el desarrollo de otras actividades.

El éxito de estas estrategias depende del grado de conocimiento y profundidad del análisis de las reacciones de cada persona, de ahí que se vincule estrechamente con el tratamiento de datos personales.

Esta peligrosa utilización del big data pone en jaque al sistema democrático como la conocemos, ya que su legitimación se basa en un proceso de información, reflexión y definición de la intención de voto de los ciudadanos, pero si la forma en que se accede a la información es involuntaria, parcial y bajo la dirección de un tercero interesado, resulta clara la manipulación indebida del electorado.

Si bien este caso ayuda a elucidar cuan necesario y delicado es regular adecuadamente la utilización de la información masiva, lo cierto es que en la actualidad existe un sinnúmero de usos y posibilidades para el big data, capaces de abrir todo tipo de escenarios y de contribuir tanto positiva como negativamente a las sociedades dependiendo de su destino, forma y regulación.

En lo que interesa a este trabajo, el big data, además, puede tener relevancia para el derecho procesal. De una parte, a través del análisis sistematizado de grandes volúmenes de sentencias judiciales se puede elaborar predicciones que permiten anticipar la decisión de los jueces, perfilar su forma de razonar frente a los casos sometidos a su conocimiento facilitando a los operadores jurídicos diseñar sus estrategias de litigación.

En la otra cara de la moneda, a través de aplicaciones de big data se han implementado sistemas que analizan grandes volúmenes de fallos, en base a lo cual elaboran proyectos de sentencias para casos "similares", algunas de las cuales podrían incluso ser aplicadas de manera automatizada a la resolución de casos sometidos al conocimiento de tribunales.

La duda razonable en este último caso es si la aplicación de este tipo de sistemas se ajustaría a los estándares del debido proceso legal y, en la afirmativa, cuáles serían los requisitos que se deben cumplir en su implementación.

Para responder estas preguntas es necesario comprender qué es el Big Data, cómo funciona y cómo puede ser utilizado, tanto de manera beneficiosa como perjudicial para las sociedades.

En nuestro trabajo abordamos diversos ámbitos que dan cuenta de los usos de la inteligencia artificial y procesamiento masivo de datos, para posteriormente centrarnos en las aplicaciones procesales, tanto en los problemas asociados a la prueba de la manipulación de la decisión de la persona como en la legitimidad del empleo de estos sistemas en la elaboración de decisiones judiciales automatizadas. Para ello haremos algunas referencias a experiencias comparadas, que permitirán visualizar una mejor solución para nuestro país.

2.- Conceptualización y revisión casuística del big data

Cuando hablamos de Big Data nos referimos a grandes volúmenes de datos, estructurados o no, que son procesados a altísimas velocidades con objeto de facilitar la toma de decisiones, resolver problemas o crear valor en múltiples ámbitos. La Agencia Española de Protección de Datos de España lo ha definido como "gigantescas cantidades de datos digitalizados que son controlados por las empresas, autoridades públicas y otras grandes organizaciones que poseen la tecnología para realizar un análisis extenso de los mismos basado en el uso de algoritmos" (Agencia Española de Poritección de Datos , 2015).

En cuanto a sus aplicaciones a la resolución de problemas de política pública, el primer caso al que nos referiremos es al de la pandemia de gripe porcina, AH1N1, que afectó a múltiples regiones del mundo el año 2009. En ese entonces, el gobierno de EE.UU., como muchos otros, se enfrentó al desafío de analizar la propagación de la enfermedad a fin de elaborar su estrategia de prevención y contención de la enfermedad. Sin embargo, los Centros de Control y Prevención de Enfermedades (CDC) no

lograban centralizar toda la información circulante a tiempo por factores como la tardanza de los pacientes en acudir a consulta sumado a que los CDC sólo tabulaban los datos una vez por semana.

En ese tiempo, un grupo de ingenieros de Google recientemente había publicado un estudio sobre cómo predecir la propagación de la gripe invernal basándose en el análisis de las búsquedas de los usuarios de la plataforma, contrastando datos y comparando una lista con los 50 millones de términos más buscados en la red con los datos de los CDC sobre la propagación de gripe de los últimos años.

El sistema diseñado por el gigante informático consistió en obtener correlaciones entre la frecuencia de ciertos términos de búsqueda y la propagación de la enfermedad. Del análisis de 450 millones de modelos matemáticos, dieron con un sistema que consideraba 45 términos de búsqueda que, al utilizarse en forma conjunta, lograba una correlación fuerte entre la predicción y las cifras oficiales de propagación al interior del país. La extraordinaria diferencia con el sistema anterior es que las predicciones comenzaron a hacerse en tiempo real, lo que tuvo como resultado una respuesta mucho más oportuna a la crisis por parte de las autoridades (Victor Mayer-Schönberger, 2013).

Otro ejemplo que nos permite aproximarnos a la comprensión de estas técnicas es el de la aplicación social de transportes Waze. El objetivo de esta compañía consiste en lograr que sus usuarios lleguen a sus respectivos destinos de manera más expedita y segura, y contribuir a la disminución de la congestión vehicular en las calles, basada en la información que aportan todos los usuarios, de manera participativa, a partir del empleo de sus GPS, comentarios, alertas y verificaciones de incidentes. El algoritmo, en este caso procesa la información y sugiere de manera personalizada, las rutas más convenientes para movilizarse en atención a los tiempos propios de la ruta, el tráfico actual, la presencia policial o de accidentes en la vía, entre otros criterios. En este caso, la eficiencia del sistema depende de la cantidad de usuarios dispuestos a entregarle datos acerca del estado de las condiciones del tránsito, de la cobertura de las redes de comunicaciones y de la calidad de procesamiento y almacenamiento de la información por parte de la empresa.

La disciplina que se aboca a diseñar e implementar estos sistemas se ha denominado “ciencia de datos”, dedicada a diseñar secuencias de procesamiento y análisis para los datos denominadas *Data Science Pipelines* o, en español, tuberías de ciencia de datos, destinadas a extraer el mayor valor posible de la información que se analiza.

Las etapas de tratamiento de la información son la adquisición, limpieza, visualización, modelamiento o análisis e interpretación de los datos obtenidos. A continuación, explicaremos brevemente un esquema de procesamiento de datos genérico, en lo que importa a nuestra investigación (Lao, 2018).

1) Adquisición o recolección de la información:

   Actualmente es posible extraer datos de todo lo que nos rodea, es decir, los colores, los niveles de resistencia de un material, la temperatura, los flujos vehiculares, los movimientos astronómicos, el desarrollo de enfermedades, las preferencias en el comercio, las personas y su comportamiento, y un larguísimo etcétera. Tratándose de la información relativa a fenómenos físicos, químicos o biológicos, puede obtenerse mediante la instalación de sensores adecuados para captar datos que permitan medir el fenómeno en estudio, tales como la captación de ondas de luz, cambio de PH, las fuerzas que se ejercen sobre una estructura, el aumento de población de una determinada bacteria, etcétera.

   Tratándose de la obtención de datos personales, en cambio, los mecanismos de obtención de datos pueden clasificarse en dos grandes conjuntos de métodos: Los métodos "activos", que se basan en la entrega de información por parte de los titulares, ya sea a través de formularios, encuestas o instrumentos semejantes, y los "pasivos", en que la información se obtiene a partir del estudio del comportamiento, con o sin conocimiento de la persona observada. En este caso se aplican métodos de *trackeo* (seguimiento) a la mera utilización de una aplicación; se utilizan "mapas de calor", que muestran la intensidad de uso en determinados puntos, o sistemas de análisis de la navegación en internet, puesto que cada vez que accedemos a internet estamos dejando un rastro de nuestro comportamiento que incluye información tal como sitios o productos de interés, lugares frecuentados, etc. Asimismo, puede recogerse información relativa a las cualidades motrices de la persona a partir del movimiento del cursor o tecleo, e incluso las emociones a partir de la observación con la cámara de las reacciones de una persona.

2) Limpieza o depuración de datos:

   Revisión de la información y eliminación de aquellos que no digan relación con el objetivo perseguido (ruido de la información).

   Esta etapa es necesaria porque los resultados del análisis (etapas posteriores del proceso) siempre van a estar condicionados a las características y calidad de los datos sobre los cuales se aplicará los algoritmos.

3) Visualización:

   Una vez depurados los datos se efectúa un primer acercamiento a las posibles conclusiones que se desprenderán del estudio, mediante la evaluación de los patrones y valores derivados de la correlación de los datos, mediante el empleo de diversos métodos de evaluación y pruebas

estadísticas cuyos resultados pueden ser representados y respaldados en tablas, gráficos u otros esquemas de organización de la información.

4) Modelamiento o Análisis:
   Los modelos, en este caso, corresponden a conjuntos de reglas expresadas por medio de algoritmos destinados a producir las conclusiones y/o predicciones del sistema o, en otras palabras, arrojar un resultado.

5) Interpretación y diseño de reportes:
   La interpretación comprende un aspecto externo al proceso, pero fundamental para su cierre y dotación de sentido. Consiste en la traducción de los datos y las conclusiones en informes comprensibles por el público al que apunta.

Otro aspecto relevante refiere a los sistemas de almacenamiento de la información que permitan procesar cantidades tan importantes de datos. Al respecto, se requiere contar con una infraestructura suficientemente robusta para el almacenamiento y procesamiento de los datos, ya sea a través de medios propios o contratando un servicio de nube o *Cloud Computing*.

Según el *National Institute of Standards Technology* (NIST), *Cloud Computing* es un modelo para habilitar el acceso a un conjunto de servicios computacionales (como redes, servidores, almacenamiento, aplicaciones y servicios) de manera conveniente y por demanda, que pueden ser rápidamente aprovisionados y liberados con un esfuerzo administrativo y una interacción con el proveedor de servicios mínimo (Peter Mell, 2011), ofreciendo la posibilidad de acceder a dicha variedad de servicios computacionales sin la necesidad de adquirir de propia mano los equipos o *softwares*, toda vez que estos son provistos de manera remota por el servidor de la nube al cual podrá accederse por vía remota desde ordenadores corrientes. Adicionalmente, la contratación de un servicio de nube supone, en la mayoría de los casos, una significativa mejora en materia de seguridad de la información puesto que, al tratarse de empresas focalizadas en el cuidado de los datos que manejan, deben garantizar altos estándares de calidad mediante la certificación de sus soportes físicos y procesos administrativos, el desarrollo o contratación de *softwares* y *firewall* adecuados, la existencia de protocolos de acceso a las instalaciones, el aseguramiento de la privacidad de los contenidos y la contratación de personal calificado para la gestión de estos y otros aspectos.

3.- Big Data e internet de las cosas *IoT*.

Otro concepto relevante es el de Internet de las cosas (“IdC”, o “IoT” por su denominación en inglés), que se refiere a la utilización de mecanismos de conexión de distintas cosas a través de dispositivos o sensores que recolectan y les transmiten información. Además de superar con creces la cantidad de habitantes del planeta, gran parte de estos dispositivos no son teléfonos inteligentes ni computadores, sino que electrodomésticos, vehículos, cámaras y toda clase de objetos dotados de sensores que pueden interactuar en la red.

A lo largo de la primera veintena del siglo XXI, la cantidad de objetos conectados a internet en el mundo aumentó drásticamente, En 2003 se contabilizaban alrededor de 500 millones de dispositivos, que subieron a 12,5 mil millones hacia 2010 (Evans, 2011), y que, previo a la pandemia, habrían llegado a más de 20 mil millones para el año 2020 (Gartner, 2017), valor que, en estas nuevas circunstancias, debiera haberse incrementado sustancialmente.

Este fenómeno de interconectividad que estamos viviendo ha transformado progresivamente la forma en que nos desenvolvemos tanto en nuestros espacios íntimos como en los lugares públicos. Casas, autos, ciudades, presumen de ser “inteligentes”, lo cual genera extraordinarios flujos de información para lograr su operatividad. En lo doméstico, la domótica permite coordinar numerosas funcionalidades del hogar desde el celular, tales como el ajuste de la temperatura y humedad, la apertura y cierre de los accesos, la limpieza, el control de las llaves de agua, la optimización de energía, la detección de movimientos en su interior o perímetro, la identificación de quienes ingresan y, más recientemente, el refrigerador inteligente que permite visualizar los productos en su interior y sus respectivas fechas de caducidad (GTD, 2019) (Samsung, 2019).

En materia de ciudades inteligentes, Tokyo, Londres, Nueva York, Zúrich, París, Santiago y Montevideo, entre muchas otras, han avanzado en la automatización de aspectos como el transporte público, luminarias, la gobernanza y planificación urbana, la optimización de generación y uso de energías, la seguridad, el medioambiente y el capital humano, entre otros. Se busca con ello aplicar modelos de planificación urbana que pongan a la persona en el centro de las políticas públicas de desarrollo urbano, puesto que ello incide de manera gravitante en la forma en que nos relacionamos como sociedad civil y con las instituciones (González, 2019).

La implementación de estas soluciones requiere de un funcionamiento armónico y eficiente de una enorme cantidad de dispositivos conectados a las redes, dotados de sensores que recolectan y procesan información de manera permanente y en tiempo real. Si bien cada artefacto mide aquellos parámetros que corresponden a su función, el conjunto de ellos permite la visualización de un panorama

mucho más completo. La gran masa de datos es sometida a algoritmos encargados de analizarlos y entregar escenarios asociados a lo que se consulte, elaborando primero un diagnóstico del estado actual de las cosas y, luego, entregando comandos de funcionamiento destinados a mantener o corregir el estado del espacio, según corresponda.

Gracias al desarrollo y masificación de las redes de sensores (WSN) que organizan los datos entre los diversos nodos sensoriales conectados, RFID para identificar los distintos instrumentos que componen el sistema por medio de ondas de radiofrecuencia, las nubes para almacenar y procesar datos, el Wifi y Bluetooth que permiten relacionar el funcionamiento de numerosos dispositivos y acceder a la red prescindiendo de cables, estándares de comunicación inalámbrica de alta velocidad como el LTE, 4G y 5G, la recolección de datos abarca prácticamente a todos los objetos y personas. Esta información se utiliza, entre muchas otras cosas, para planificar un gasto eficiente de energías, por ejemplo aumentando o bajando su intensidad dependiendo de si hay o no transeúntes en una calle; crear y monitorizar programas de deporte y vida saludable, para prevenir enfermedades; estudiar los flujos vehiculares y peatonales que permitan organizar el sistema de transporte público, los flujos y recorridos; aumentar la capacidad de respuesta ante emergencias; monitorear de manera permanente las condiciones ambientales, junto con una toma eficiente de medidas preventivas y correctivas, y la intervención directa de la ciudadanía en la toma de decisiones que afecten su localidad (Ibrahim Abaker Targio Hashem, 2016). Otro de los efectos positivos de las ciudades inteligentes se asocia a la transparencia y acceso a los datos que se recogen en sistemas de gobernanza abiertos, de forma tal que sea factible la reutilización de dicha información para crear valor público o privado.

En contraste con las experiencias electorales expuestas de Brasil y EE.UU, el Big Data puede utilizarse en pos del fortalecimiento de los sistemas democráticos. De ello concluimos que los riesgos asociados a determinados tipos de herramientas o tecnologías no son inherentes a las mismas, sino que son los usos que decidan hacer de ellas sus creadores o usuarios los que determinarán su bondad.

El mundo empresarial también utiliza el Big Data en la gestión de negocios, bajo la denominación de *Data Driven*. Esto es, modelos de adopción de decisiones basados en la interpretación de datos.

Entre las aplicaciones destacan la optimización de sus procesos productivos y prácticas comerciales, estudios de mercado, análisis de modelo de servicios, la creación de nuevos productos, para adecuarse a los nuevos requerimientos de la compañía y su público. En este nuevo modelo de negocio los datos son un recurso clave y las decisiones se adoptan a partir de la ampliación y diversificación de sus fuentes de datos, sumado a la aplicación de metodologías de análisis de datos que le permiten

comprender a cabalidad el complejo esquema de efectos y correlaciones que inciden en el desarrollo de su negocio.

Las dimensiones que caracterizan el *Data Driven* son:

1) **Recursos clave:** Son todas las herramientas, pertenencias, atributos, información, conocimiento y capacidades de la firma. Para este modelo es importante destacar los datos, distinguiendo aquellos que se obtienen de fuentes externas a la compañía de los que se generan internamente gracias al procesamiento de dicha información.
2) **Actividades clave:** Todas las prácticas destinadas a la obtención del producto que se ofrece. Para efectos de los datos, en esta categoría se encuentran funciones como la selección de información, su limpieza, análisis, identificación de patrones, entre otras operaciones.
3) **Propuesta de valor:** Valoración de los clientes en base a su experiencia. Al igual que muchos aspectos del negocio, la experiencia de los clientes igualmente puede ser datificada, lo que constituye otra base de datos a ponderar en busca de mejoras.
4) **Segmento de clientes:** Corresponde al público al que apuntan los productos o servicios de la empresa. Se debe analizar su desempeño en relación con este público y también sus características para ofrecer publicidad y servicios personalizados.
5) **Modelo de ingresos:** Marco de generación de ganancias que identifica los distintos pasos, ámbitos y actores generadores de ganancias para la compañía. Esta información contribuye significativamente a la fijación de precios de los productos y/o servicios que se ofrecen. Mientras más datos se tengan para ello, mejores probabilidades hay de llegar a un resultado óptimo.
6) **Estructura de costos:** A contracara, la estructura de costos determina los puntos de fuga de capital, desde la compra de insumos, el pago de remuneraciones, los costos energéticos y productivos, etc. Tal como ocurre con los ingresos, lograr un paneo detallado de estos aspectos y analizarlos de manera conjunta, contribuye de manera gravitante en la comprensión del esquema de producción y puede aportar significativamente en su optimización.

El levantamiento y comprehensión de toda esta información entrega un panorama de funcionamiento de altísimo valor para la empresa, toda vez que proyecta el proceso completo, permite su optimización y facilita la toma de decisiones en su interior (Philipp Max Hartman, 2016).

4.- Machine Learning o aprendizaje automático.

Los grandes avances en estadística, la mayor tecnificación de los algoritmos, el descomunal incremento en los volúmenes y tipología de datos existentes y el aumento de la capacidad computacional

de los sistemas de procesamiento han permitido el desarrollo de técnicas de Inteligencia Artificial cada vez más complejas, toda vez que al sistema de comandos e instrucciones realizables por una máquina se agrega la creación de métodos que posibilitan la detección automática de patrones en los datos analizados, permitiendo una mejora simultánea de sus propios algoritmos, lo que, en definitiva, facilita la elaboración de predicciones y la toma de decisiones cada vez más precisas.

Existen diversas técnicas y formas de modelamiento de la información para lograr que el sistema aprenda. Encontramos modelos de aprendizaje supervisado y de aprendizaje no supervisado. En el primero, el algoritmo con que se programa la máquina contiene información sobre la característica particular que se quiere estudiar, de modo que se entrena el sistema, por ejemplo, mostrándole un set fotográfico de gatos a fin de que entienda qué es lo que tienen todas ellas en común para que en el futuro cuando se le presenten imágenes de animales diversas a las originales, el algoritmo pueda poner en práctica sus conocimientos y concluir si es que entre ellas hay o no alguna figura asemejable a lo que se entiende como gato. En cambio, en los modelos de aprendizaje no supervisados no se incluye entre los datos de programación del algoritmo una muestra que contenga la variable que se pretende estudiar, de tal manera que, replicando el ejemplo anterior, cuando se elabora el programa no se incluyen imágenes de gatos; así, cuando se le presenten las figuras de diversos animales, el algoritmo tendrá la labor de identificar los patrones comunes entre ellas y armar correlaciones de datos para clasificar y comprender lo que se le presenta (Management Solutions, 2018).

Entre las técnicas de aprendizaje automático se encuentran:

1) **Redes Neuronales:** Modelos no lineales cuyas conexiones de pequeños nódulos imitan los sistemas nerviosos biológicos mediante procedimientos iterativos que apuntan a la minimización de una determinada función de error en el proceso de análisis.
2) **Máquinas de vector de soporte:** Modelos de clasificación para muestras de datos complejos.
3) **Clasificadores Bayesianos:** Modelos que utilizan la información conocida que se ha incorporado al algoritmo con objeto de clasificar sus observaciones.
4) **Árboles de clasificación:** Modelo que clasifica la muestra en grupos predefinidos. Es un sistema sencillo, pero más limitado que los demás.

En particular, las redes neuronales han experimentado un excepcional desarrollo en lo que va del siglo gracias al trabajo de investigadores y desarrolladores como Geoffrey Hinton, Yan LeCun y Yoshua Bengio, quienes fueron recientemente reconocidos con el Premio Turing, certamen que se ha dado a conocer como “El Nóbel de la Informática”, por sus importantes contribuciones al Deep Learning (Limón, 2019).

El Deep Learning, o aprendizaje profundo, es una variante de las redes neuronales caracterizada, según los propios galardonados, por la capacidad de analizar múltiples niveles de representación al trabajar con un formato de análisis no lineal. En otros términos, esta modalidad de procesamiento de información imitativo del cerebro humano posee la virtud de extraer conclusiones respecto de la muestra con distintos niveles de abstracción, lo cual le permite comprender con mayor complejidad y profundidad las cualidades de la información de que dispone.

Los investigadores afirman que, desde esta vereda, se están haciendo grandes avances en ámbitos que requieren del estudio de estructuras multidimensionales, lo que tiene aplicaciones concretas en áreas como el desarrollo comercial y gubernamental, en el notable perfeccionamiento que han experimentado los sistemas de reconocimiento de imágenes y sonidos, los sistemas de traducción de idiomas, la predicción de los efectos por ingesta de drogas y fármacos, el estudio de los datos que arroja el acelerador de partículas, la reconstrucción de circuitos cerebrales y la predicción de efectos de mutaciones sobre el ADN. Así, el éxito que prometen estas tecnologías se debería, en gran medida, al hecho de que su desarrollo requiere de muy poca "ingeniería de mano", ocupando los desarrolladores un espacio bastante pequeño para el aprendizaje de estos sistemas en relación con el rol que desempeñan los grandes volúmenes de datos que estos deben analizar (Geoffrey Hinton, 2015).

Nos detuvimos en el *Deep Learning* puesto que, si bien corresponde a un área de procesamiento de la información con un extraordinario potencial de desarrollo, ya en la actualidad está generando importantes efectos sobre diversas áreas del conocimiento y sobre la información relativa a miles de millones de personas en el mundo. Esta afirmación se vuelve mucho más tangible si se tiene en cuenta que Hinton, LeCunn y Bengio trabajan en los sistemas de Deep Learning con que funcionan Google, Facebook, IBM y Microsoft para comprender las implicancias de las búsquedas de los usuarios, mejorar el reconocimiento físico de las personas a partir de las fotografías que se suben a las redes sociales, mejorar el perfilamiento de los ciudadanos y segmentación de las personas para personalizar los contenidos que se les ofrece y la publicidad que se les entrega, entre muchas otras funciones. Asimismo, Apple, Amazon y, en general, los gigantes de la información utilizan algoritmos de Deep Learning para mejorar sus productos y servicios, repercutiendo de igual manera en la vida de quienes los utilizan.

Como hemos visto, el Big Data atraviesa la mayor parte de las áreas de desarrollo humano moderno y puede ser utilizado tanto con fines tremendamente beneficiosos como perjudiciales para las personas y los entornos en que se desarrollan las comunidades.

5.- Los usos procesales del big data.

Habiendo abordado diversas formas de su funcionamiento, es momento de adentrarnos en los usos procesales actuales y potenciales del big data.

Los sistemas judiciales, tan largamente criticados por su lentitud, el estanco de los procedimientos, su tradicionalismo e híper burocratización, no están exentos de poder perfeccionar su funcionamiento y agilizar su labor por medio de la implementación de mecanismos de procesamiento masivo de datos en distintas áreas del proceso o bien de su funcionamiento interno. Sin embargo, lo que resulta particularmente delicado es la sensibilidad que reviste esta función del Estado para cada entidad involucrada y para la comunidad toda. Por esta razón, la lógica de aplicación no puede tener como objetivo único la optimización de los procesos, sino también, y con igual o mayor importancia, el que dicha optimización resguarde en todo momento y maximice la protección de los derechos de los involucrados y su intimidad. Los próximos capítulos darán cuenta de cómo abordar tales conflictos. Por lo pronto, atenderemos algunos de los posibles usos procesales del big data.

Entre los problemas que destacan en los actuales sistemas de tramitación de causas y cuyas soluciones son abordables con herramientas de big data e inteligencia artificial se encuentran (Ariel Podestá, 2019):

- La falta de un sistema centralizado que permita revisar todos los antecedentes de un caso de manera ordenada.[1]
- La necesidad de normalizar e integrar la información de los múltiples documentos que se obtienen en toda índole de fuentes y formatos, que vuelve difícil su análisis. Para ello se requiere el establecimiento protocolos de entrega de información que estandaricen su forma de análisis.
- La dificultad de conocer la trazabilidad completa de la información, cuya fuente originaria muchas veces se desconoce, lo que complejiza la determinación de su fiabilidad.
- El aseguramiento de la confidencialidad y seguridad de los datos. Aspecto de gran relevancia a efectos de cuidar la privacidad, integridad física y psíquica de las personas y de resguardar la presunción de inocencia.
- La falta de sistemas de análisis que logren establecer vínculos y relaciones entre los datos en estudio y que podría facilitar y acelerar determinados aspectos de una investigación.

Esta capacidad de establecer vínculos a lo largo y ancho de todas las investigaciones o causas contenidas en el sistema, así como de las pruebas aportadas en ellas, podría facilitar significativamente

[1] Situación que se ha resuelto significativamente en Chile gracias a la digitalización de los expedientes y el desarrollo de la Oficina Judicial Virtual (OJV).

la obtención de información adicional y conclusiones que no siempre son percibidas por los operadores a la hora de estudiar los expedientes uno a uno y página por página. Por ejemplo, si a partir del estudio de una causa el sistema arrojara todos los expedientes en que se ha visto involucrado un mismo nombre, vehículo, arma o *modus operandi* sería mucho más probable abordar los fenómenos de manera global, ahorrando tiempo, duplicidad de trabajo y aumentando las opciones de una investigación exitosa.

Sin perjuicio de lo anterior, es posible también aplicar técnicas de big data a los sitios de búsqueda y análisis de información jurídica con el objeto de facilitar y diversificar los usos de los repositorios, se puede implementar sistemas que busquen correlaciones y ordenen adecuadamente el material probatorio a presentar, o bien sistemas de llenado automático de documentos tipo, como resoluciones básicas a las que falta agregar los datos de la causa o resoluciones que solicitan el mismo tipo de información a numerosas instituciones y que requieren del cambio de datos específicos en su redacción.

Asimismo, se está trabajando hace algunos años en mecanismos de predictibilidad de fallos judiciales que ayuden a conocer las tendencias decisionales de los distintos tribunales en relación con temas determinados. Por lo pronto hay sistemas que han apuntado al ámbito resolutivo de las sentencias y no a su parte considerativa, logrando un margen de acierto significativo respecto del "acoge" y "rechaza", como ocurre con un algoritmo desarrollado para predecir las decisiones de la Corte Suprema de Estados Unidos (Daniel Martin, 2016), mientras que otros, como Prometea en Argentina, han sido más ambiciosos e intentado abarcar de manera más íntegra el entramado de información y funciones que pudieran resultar útiles para la aplicación de justicia, incluyendo la revisión de casos similares, la resolución de casos en base a la jurisprudencia y la redacción de propuestas de dictámenes que resuelven determinados conflictos en base a precedentes judiciales reiterados. En este sentido, cabe destacar que en la actualidad Prometea se está utilizando tanto en el Ministerio Público Fiscal de Buenos Aires como en la Corte Interamericana de Derechos Humanos a modo de apoyo para resolver y para acelerar la resolución de tareas repetitivas (Universidad de Buenos Aires, 2020) (Elsa Esteves, 2020).

También comienzan a ganar terreno los contratos inteligentes que se han podido desarrollar gracias a la programación en bloques, *blockchain*, y que IBM define como "programas almacenados en una cadena de bloques que se ejecutan cuando se cumplen condiciones predeterminadas", permitiendo automatizar de inmediato el cumplimiento de acuerdos entre partes sin necesidad de pérdidas de tiempo ni intermediarios. Básicamente se trata de programar una condición y una acción en caso de cumplirse o no dicha condición. Bajo este esquema se puede "liberar fondos a las partes apropiadas, registrar un vehículo, enviar notificaciones o emitir un boleto" (IBM, 2022), dando celeridad a los procesos y la confianza de que no es un tercero eventualmente parcial el encargado de resolver en base al cumplimiento de la condición. La posibilidad de dar cumplimiento inmediato a los contratos, como en este caso, bien

puede disminuir la carga judicial de las causas referidas a la interpretación de contratos y, especialmente, de su cumplimiento forzoso.

6.- Riesgos asociados al tratamiento de datos masivos:

Una de las primeras preguntas que plantea esta materia es si acaso el tratamiento de datos masivos representa exactamente los mismos riesgos que cualquier tratamiento de datos, pero en un grado más alto, o si la utilización de este tipo de procesos y tecnologías conlleva riesgos adicionales.

La pregunta es importante, puesto que, si sólo se trata de los mismos riesgos, pero aumentados, bastaría con mantener las formas de regulación tradicionales y simplemente implementarlas con mayor intensidad; en cambio, si los problemas que se generan son diversos, resulta necesario replantearse las políticas regulatorias de modo que puedan abordar los efectos que conlleva este fenómeno en su conjunto.

Para Viktor Mayer-Schönberger y Kenneth Cukier la posibilidad de tratar datos masivos ha transformado el problema, toda vez que el valor de la información ya no reside sólo en su propósito primero, sino también en sus usos secundarios. Según exponen los autores, la finalidad de estos usos secundarios, por lo general, no ha sido siquiera ideada al momento de la recopilación de la información, lo que supone un cambio muy significativo en el modelo del consentimiento informado y, por tanto, en el rol que deben jugar los titulares frente al tratamiento de sus datos (Victor Mayer-Schönberger, 2013).

Uno de los riesgos más notorios y reiterados del tratamiento masivo de datos refiere al temor fuertemente instalado durante el siglo XX respecto de los sistemas de inteligencia gubernamentales empleados por los Estados policiales característicos de la guerra fría y tan bien retratados por las distopías de autores como Orwell y Bradbury.

Las sociedades contemporáneas, más bien liberales, temen al fantasma de los Estados autoritarios e intrusivos. Aunque dichos temores se fundan razonablemente en la experiencia histórica, corresponde realizar un alcance, y es que, en la actualidad, el potencial de control y dominación dirigida y personalizada de las sociedades no se limita únicamente al manejo de información por parte de los Estados, sino también de las grandes corporaciones que gozan de presencia mundial. La globalización ha tenido como correlato el megalómano crecimiento de ciertas empresas que se han caracterizado por absorber toda índole de industrias y por superar con creces las regulaciones de sus países de origen para llegar a convertirse en una suerte de Estados sin fronteras capaces de determinar, en base a su descomunal

dominio de los mercados, los términos de quienes "habitan" en ellos, vale decir, de su público objetivo y, en general, de las esferas que los rodean, puesto que, además, logran influir significativamente en la determinación de las políticas públicas de los Estados en base al lobby y a su gran poder negociador.

Otro factor de riesgo dice relación con el altísimo poder de mercado que acaparan gigantes tecnológicos, como Google, Facebook, Amazon, Microsoft e IBM, entre otros. El grado de poder económico y la cantidad de datos que recopilan estas compañías cada segundo de cada día es tan impresionante que vuelve prácticamente imposible la competencia por parte de las Start-Ups que, en último término, acaban por apostar a que estos gigantes compren y absorban sus buenas ideas.

Uno de los puntos que planteará el último capítulo de este trabajo será el impacto que tiene la recogida y concentración de grandes cantidades de información para la salud de los mercados en relación con la Libre Competencia.

No conforme con ello, y como veíamos al comienzo de este capítulo, la utilización masiva de datos también puede poner bajo amenaza los sistemas democráticos como los conocemos, pues, en la medida que existan entidades, tanto públicas como privadas, capaces de sobre determinar el acceso que tiene la ciudadanía a la información, e incluso a la desinformación, se diluye por completo la potestad y racionalidad de los pueblos para elegir y ejercer un control efectivo sobre las acciones y decisiones de sus gobernantes, así como para pronunciarse acerca de las relaciones que estos puedan establecer con determinados grupos de poder.

Asimismo, resultan problemáticos los sesgos discriminatorios que se puede imprimir a los sistemas de procesamiento masivo de datos e inteligencia artificial y que ya han sido fuertemente cuestionados en el campo del reconocimiento facial.

Para ejemplificar, el año 2016 tuvo lugar un gran escándalo en Estados Unidos cuando la Oficina de Accountability del Gobierno norteamericano (GAO) hizo público que desde el año 2011, y en secreto, el FBI se dedicó a recolectar y tratar imágenes de más de la mitad de los adultos del país sin previo aviso y con el fin de monitorear su comportamiento de manera permanente mediante dispositivos de reconocimiento facial emplazados en numerosas ciudades del país (United States Government Accountability Office (GAO), 2016).

Por si no fuera suficientemente grave la obtención ilegítima de estas imágenes, muchas veces tomadas de las licencias de conducir y otros documentos oficiales generados para fines diversos, y su posterior utilización para vigilar a la población de manera oculta, sin rendir cuenta de estos procesos y transgrediendo la presunción de inocencia[2], resultó que la alarma derivada de esta situación dio lugar a

[2] Garantía de que no se puede investigar a una persona sin que exista indicios de la comisión de un delito.

una serie de investigaciones y auditorías que concluyeron que los sistemas utilizados padecían de importantes sesgos discriminatorios que tendían a generar una mayor cantidad de falsos positivos en contra de la población afroamericana, de género femenino y de edad avanzada.

La evidencia científica a la fecha afirmaba que los sistemas de reconocimiento facial tienden a replicar los sesgos con que son entrenados (Klare, Burge, Klontz, & Jain, 2012). De modo que estos sesgos no son inherentes al procesamiento masivo de imágenes, sino que responden a factores externos, como sus mecanismos de entrenamiento. Si un sistema es entrenado con una muestra de fotos en que predominan los hombres caucásicos de mediana edad, será muy probable que el software aprenda a distinguir muy bien entre ellos, pero podría presentar mayores problemas a la hora de identificar personas de otra raza, género o grupo etario.

En el caso norteamericano, la realidad es que la población afroamericana tiene un mayor contacto con las fuerzas de seguridad, lo que, a su vez, deriva en una mayor tasa de detenciones que fácilmente pueden llevar a un sistema de inteligencia artificial a concluir que existe una probabilidad mayor de criminalidad en la población que comparte este rasgo. Si a este hecho se suma que los sistemas tienden a cometer más errores cuando se analizan imágenes de afrodescendientes, queda en evidencia una preocupante tendencia a criminalizar en forma equívoca a persona pertenecientes a este segmento de la población (Garvie, Bedoya, & Frankle, 2016).

Lo propio se ha visto en sistemas de inteligencia artificial aplicados en Estados Unidos para el apoyo de las sentencias, donde se han denunciado sesgos raciales del programa Northpointe respecto de las probabilidades de reincidencia de los sujetos penales (Julia Angwin, 2016), lo que puede conllevar la denegación de beneficios carcelarios, problemas significativos para la reinserción e incluso la aplicación de penas superiores, constituyendo un significativo agravio al principio de igualdad ante la ley, la presunción de inocencia, al debido proceso y al acceso a la justicia, quitando de paso legitimidad a las instituciones encargadas de impartir estas decisiones, especialmente en países como el propio Estados Unidos con tales magnitudes de población penal y donde la mayor parte de esta es efectivamente afrodescendiente.

Aunque el algoritmo cuestionado no incluía preguntas como el origen racial de los involucrados, sí contenía interrogantes acerca de la incidencia penal de los entornos familiares, la relación con drogas de los entornos sociales y otras de similares características que, en sociedades donde un segmento social determinado fenoménicamente tiene más contacto con la criminalidad, pueden llevar al sistema a concluir que dicho segmento social tiene probabilidades mayores de incidencia, lo que, si bien no es un ataque directo contra el segmento social *per se*, sí puede perjudicarle al momento de aplicar tales consideraciones en una sentencia judicial.

Así queda claro que para afrontar este tipo de riesgos se debe ser muy cuidadoso a la hora de entrenar los sistemas de análisis y también ejercer un control permanente de sus resultados y formas de funcionamiento, de manera que puedan evitarse los sesgos derivados del entramado de procesos que ocurren en su 'caja negra'. En otras palabras, sigue siendo fundamental la aplicación del criterio humano y la supervisión de todos los procesos entregados a los sistemas de procesamiento automatizado de datos.

En un plano distinto a la mera manipulación de datos, pero no menos importante, se encuentran los riesgos asociados a la cibercriminalidad.

Como era de esperar, un salto tecnológico de esta envergadura en todas las esferas de relacionamiento social tenía que traer consigo un salto de similar magnitud en los mecanismos de ataque a la integridad de dichas formas de relacionamiento y a las herramientas e instituciones que las hacen posibles.

En la actualidad vivimos una escalada muy significativa de la cibercriminalidad, que se ha visto más intensificada gracias a las condiciones de vida y trabajo forzadas por las cuarentenas en el mundo entero. El hecho de que toda la información que manejamos se encuentre en línea y la gran cantidad de tiempo que pasamos conectados a la red constituyen un aliciente para quienes buscan dañar los sistemas operativos de diversas empresas o instituciones, acceder a datos críticos o enriquecerse a partir de la apropiación de datos de terceros y su posterior amenaza de eliminación.

Para evidenciar la magnitud que pueden llegar a lograr este tipo de ataques, parece útil destacar un caso que, no obstante, su gravedad, logró pasar relativamente desapercibido, a saber, el secuestro cibernético de los sistemas de datos de Baltimore que tuvo lugar a mediados de 2019 y cuyas consecuencias son palpables hasta el día de hoy.

El 7 de mayo de 2019 los sistemas de información de la ciudad estadounidense fueron *heackeados* por un programa malicioso. El ataque imposibilitó la utilización de las herramientas e información necesarias para el normal funcionamiento de los diversos establecimientos y servicios que componen el entramado urbano y, no conforme con ello, inhabilitó los accesos a cuentas, facturas y sus respectivos mecanismos de pago para la totalidad de la población. Tras el ataque, los perpetradores se comunicaron y exigieron el pago de 13 Bitcoins – alrededor de US$100.000 - para liberar la información y sus sistemas de procesamiento. Sin embargo, las autoridades se rehusaron a negociar y, con objeto de no promover la actividad criminal, declinaron la oferta de rescate asumiendo que sus equipos de contrainteligencia podrían dar con una solución en el corto plazo; error que conllevó un gasto millonario para el Condado de Baltimore y un molesto viaje en el tiempo de vuelta a la era analógica. Durante meses los ciudadanos debieron efectuar sus trámites de manera presencial, tardando más de 2 horas en largas filas generadas para el pago de cada cuenta de servicios.

Dado que en la actualidad la mayor parte de los pagos por servicios se hace en línea, las empresas proveedoras ya no cuentan con los sistemas ni con el personal suficiente para atender a la totalidad de sus abonados en forma presencial, circunstancia que llevó al colapso de la urbe durante el período posterior al ataque. Por si fuera poco, a un mes del evento, una gran cantidad de sistemas seguían secuestrados, se había incurrido en un gasto de US$4,6 millones y se estimaba que el condado debería desembolsar un total de US$18,2 para reestablecer por completo sus sistemas operativos (Laborde, 2019).

Este evento, tremendamente grave por sí solo, evidencia dos importantes vulneraciones a los sistemas de ciberseguridad norteamericanos: La primera y más notoria corresponde al ataque perpetrado contra los sistemas informáticos de Baltimore; la segunda, ocurrida con antelación, fue dada a conocer por el New York Times cuando el secuestro del condado cumplía 3 semanas: Según el periódico, la herramienta utilizada para inhabilitar los sistemas con tal efectividad correspondía a un proyecto que aprovechaba una brecha de seguridad de Windows, que había sido desarrollado por la Agencia Nacional de Seguridad (NSA) y financiados por los impuestos de los propios ciudadanos que se vieron afectados por su utilización. El nombre del *malware* era "EternalBlue" y habría sido sustraído de la NSA el año 2017, siendo presuntamente utilizado con posterioridad para llevar a cabo ataques no solo en Baltimore, sino también en Korea, Rusia, China, en hospitales, aeropuertos, fábricas de medicamentos críticos, entre otras instituciones sensibles para la comunidad. Aunque la NSA y el FBI no se refirieron a la situación, algunos expertos en ciberseguridad y empleados de la NSA dieron cuenta de estos hechos (Perlroth & Shane, 2019).

Independiente de si llega o no a comprobarse que el programa pertenecía a la NSA y que fue sustraído el año 2017, lo que se pretende hacer notar en estas líneas es la magnitud del daño que puede llegar a producirse en las personas, las instituciones y la forma de cotidianeidad y relacionamiento de las comunidades por medio de ataques que exploten las vulneraciones de los sistemas en línea, más aun bajo el entendido de que prácticamente toda la información que utilizamos se encuentra en la red.

Las fallas o la desatención de los sistemas de ciberseguridad pueden tener consecuencias catastróficas y es por esto que las materias relacionadas con la seguridad informática y la ciberdelincuencia adquieren un peso gravitante en la consideración de los riesgos derivados del tratamiento masivo de datos.

CAPÍTULO II: Regulación del Big Data y análisis de aplicaciones procesales en base a la normativa europea, chilena y el caso de Estonia.

Habida cuenta de los riesgos asociados al tratamiento masivo de datos, este capítulo tiene por objeto profundizar en las respuestas regulatorias que se han dado desde la Unión Europea, abordando en particular el caso de Estonia y revisando el escenario chileno actual junto con sus perspectivas de desarrollo normativo próximo.

Para ello, los principales instrumentos a revisar son el Reglamento General de Protección de Datos (RGPD) de la UE en relación con la ley 19.628 sobre Protección de la Vida Privada y el proyecto de ley de protección de datos personales que se encuentra actualmente en tramitación, por un lado, y, por otro, el Convenio de Budapest, también de la UE, en relación con la ley 19.223 sobre Delitos Informáticos y el proyecto de ley de delitos informáticos que busca derogarla para modernizar la tipificación y persecución penal de estos ilícitos.

Respecto de la normativa estonia, dada su pertenencia a la UE aplica el mismo RGDP y, adicionalmente, el Acta de Protección de Datos Personales, cuya versión más reciente rige desde enero de 2019.

1.- Regulación Civil del Big Data

a) Breve revisión de la evolución normativa en la UE:

Sin lugar a dudas, la primera zona geográfica que dio cuenta del problema y trató de adelantarse a sus consecuencias fue la Unión Europea (UE) que, desde la década de los ‘60, paralelo al desarrollo de mecanismos de automatización de procesamiento de información, comenzó a normar la utilización de los datos personales, estableciendo requisitos y limitaciones para su empleo. Este impulso desembocó en la creación del Convenio sobre Datos Personales del Consejo Europeo de 1980 que constituyó el primer intento de unificación normativa en la materia para el viejo continente. Luego, en 1995, el Consejo Europeo logró la aprobación de la Directiva de Protección de Datos Personales, instrumento jurídico que

sentó un importante precedente en el mundo, toda vez que la UE obligó a sus Estados miembros a adoptarla e impulsó también su incorporación en países ajenos que podían motivarse a elevar sus estándares de protección en aras a lograr mejores relaciones comerciales (Revista Chilena de Derecho Informático, 2003).

Los vertiginosos avances en las esferas de la tecnología e información que siguieron a la aprobación de esta Directiva la llevaron a una pronta desactualización, por lo que el 25 de mayo de 2018 comenzó a regir el Reglamento General de Protección de Datos (RGPD), instrumento mucho más acucioso que los anteriores, que, igualmente, tiene un carácter obligatorio para todos los países miembros de la UE pero que, además, ha sido adoptado voluntariamente por gran parte de las empresas transnacionales relacionadas al rubro de las tecnologías que operan a nivel internacional.

Un aspecto interesante de este reglamento es que, si bien se preocupa de elevar los niveles de protección sobre los datos personales y aumenta las sanciones asociadas a la vulneración de la privacidad de sus titulares, lo hace con miras a armonizar el desarrollo de las industrias tecnológicas e informáticas con el blindaje que otorga a la protección de la información. En otras palabras, estamos frente a un cuerpo normativo que entiende que, en el mundo de la información que vivimos, los datos constituyen un activo y una herramienta tremendamente relevante para toda índole de actividad económica, servicios y prestaciones sociales, pero que, al mismo tiempo, se preocupa de evitar que dicha circunstancia sea una excusa plausible para vulnerar la esfera íntima de las personas y su autonomía informativa. Bajo esta lógica, el RGPD innova en la regulación del Big Data proponiendo los aspectos que revisaremos a continuación.

Hasta la entrada en vigencia de este instrumento, el paradigma del tratamiento de datos personales era el consentimiento de sus titulares, de modo que, para poder procesar este tipo de información de manera legítima, las instituciones debían informar a los titulares acerca de los datos que iban a obtener junto con los usos y fines que pretendían darles. Luego, ya autorizados por el titular, sólo podían tratar la información en conformidad a lo que hubiera sido informado y autorizado. Así, cualquier forma de tratamiento dentro de este marco era responsabilidad del titular que accedió.

El RGPD rompe con esta lógica al comprender que, en la actualidad, es tremendamente difícil e inoficioso contar con una autorización explícita para cada dato y cada forma de tratamiento que se le pretenda dar, por lo que consagra mecanismos diversos de validación del uso de la información, por un lado, traspasando la responsabilidad desde el titular a la entidad dedicada al procesamiento de la información, debiendo esta encargarse de velar por el cumplimiento de todas las garantías que establece el reglamento, y por otro lado, legitimando la posibilidad de dar segundos usos a la información sin contar con el consentimiento explícito del titular siempre que se cumplan los requisitos dispuestos por la

ley. Estas modificaciones tienen consecuencias de suma relevancia, como son la flexibilización del principio de finalidad, que había trascendido a los sistemas anteriores, y la consolidación de una nueva base de licitud para el tratamiento de la información personal.

No es difícil evidenciar que semejante transformación al modelo resulta favorable para las empresas que durante años se han enriquecido gracias al tratamiento indiscriminado de datos personales, puesto que vuelve todavía más sencilla la obtención de la información y amplía las alternativas de justificación para validar dicha captación. Sin embargo, un breve análisis del escenario anterior puede dar cuenta del motivo de esta modificación, especialmente si se tienen en cuenta aspectos como la escasa cultura de la privacidad hasta ahora desarrollada por la mayor parte de la población, el persistente condicionamiento por parte de aplicaciones móviles y sitios web que sólo permiten a los usuarios aprovechar sus respectivos servicios a cambio de conjuntos de datos que no dicen relación con la prestación en cuestión y, por cierto, el hecho de que para las empresas e instituciones públicas es más fácil que para las personas obtener asesoría legal y sistemas de gestión que se adapten a las nuevas normativas.

Ya en el año 2014 el Grupo de Trabajo del artículo 29 (WP29), sostenía la existencia de una fuerte convicción en que los principios de protección con que contaba la UE, tal como los establecía la Directiva 95/46/EC, no resultaban válidos ni apropiados dado el grado de desarrollo del Big Data. Estas consideraciones, decían, serían un aspecto clave en la creación y mantenimiento de la confianza en el desarrollo de un modelo de negocios estable basado en el procesamiento de información personal. Asimismo, creían que un sistema de cumplimiento investido de soluciones amigables con la privacidad sería esencial para asegurar una competencia efectiva entre los diversos agentes económicos, especialmente para que las compañías que hubiesen logrado construir monopolios o posiciones dominantes previo al desarrollo de tecnologías de Big Data no mantuvieran esta ventaja respecto de los nuevos competidores (Article 29 Working Party (WP29), 2014).[3]

En todo caso, vale la pena señalar que este modelo no llega a suponer una carta en blanco para las entidades que se dedican al procesamiento de datos personales, pues tanto la flexibilización del principio de finalidad, como la legitimación de segundos usos de la información, para ser viables, deben cumplir con una serie de requisitos cuya inobservancia acarrea importantes sanciones de carácter económico y administrativo que pueden consistir en la suspensión del flujo de datos y llegar a 20.000.000 de Euros o

[3] "In fact, the Working Party strongly believes that complying with this framework is a key element in creating and keeping the trust which any stakeholder needs in order to develop a stable business model that is based on the processing of such data. It also believes that compliance with this framework and investment in privacy-friendly solutions is essential to ensure fair and effective competition between economic players on the relevant markets. In particular, upholding the purpose limitation principle is essential to ensure that companies which have built monopolies or dominant positions before the development of big data technologies hold no undue advantage over newcomers to these markets."

al 4% del total de ganancias del período anterior, pudiendo optar por la de mayor cuantía, constituyendo así un importante incentivo en orden al cumplimiento de las disposiciones del reglamento.

b) Contexto Regulatorio en Chile:

Chile cuenta con una ley de protección de datos desde el año 1999. Como se puede inferir, en aquella época, este hecho constituyó un gran avance en nuestra legislación, convirtiéndonos en un país de avanzada en la materia al dar este salto cuando la Directiva 95/46/EC de la UE recién había entrado en vigencia. Sin embargo, la Ley 19.628 sobre Protección de la Vida Privada, cuyo objeto principal era normar los nuevos sistemas de tratamiento de datos comerciales que, por entonces, y hasta la actualidad, afectan de manera tan sensible el quehacer económico y financiero de grandes segmentos de la población, no logró aplicarse como se esperaba. Aunque establecía principios y parámetros razonablemente adecuados para la época, lo cierto es que los distintos actores jurídicos y administrativos no supieron explotar las funciones y beneficios de esta nueva norma.

Los principios bajo los que se reguló el tratamiento de datos personales fueron la libertad para tratar esta información conforme a la ley, los principios de información y consentimiento, el principio de finalidad, la calidad de los datos, el establecimiento de un estatus diferenciado para el tratamiento de datos sensibles y la relevancia de la seguridad de los datos personales que son tratados.

A su vez, esta ley consagró para todas las personas naturales los Derechos ARCO, a saber, Acceso, Rectificación, Cancelación y Oposición que, respectivamente, permiten al titular de la información acceder a ella, esto es, saber quién tiene qué información sobre su persona; rectificar o corregir esta información cuando sea equívoca o se encuentre desactualizada; cancelar o bloquear esta información, vale decir, exigir su eliminación de las bases de datos que la contengan sin expresión de causa y la facultad de oponerse a los usos que se le estén dando a sus datos en un momento determinado.

La ley 19.628 estableció un procedimiento especial para conocer y sancionar los asuntos relativos al tratamiento de datos personales conocido como *Habeas Data,* o Amparo de los datos, por su similitud con las acciones cautelares previstas en la constitución, especialmente aquella prevista para exigir que se ponga ante la justicia a quien se hallare amenazado o detenido de manera ilegítima a fin de resguardar sus derechos a la libertad personal y seguridad individual. El objetivo del Amparo de los datos era – y sigue siendo- que cualquier persona, en calidad de titular de su propia información, pudiera requerir de todo responsable de una base de datos personales dedicado a su tratamiento y que contenga su información, que se le documente acerca de su procedencia, destinatarios, el propósito de su

almacenamiento, los organismos a los que se remiten estos datos con regularidad, así como también para exigir su modificación, eliminación o bloqueo atendiendo a la calidad de la información, o bien, en virtud del respeto y protección debidos a los datos personales.

No obstante, este procedimiento, ideado como uno sumamente sucinto, se entregó a la competencia de los Tribunales civiles ordinarios, órganos particularmente lentos en la tramitación de causas. Como si aquello no fuera un desincentivo suficiente, para poder accionar de *Habeas Data* es necesario el patrocinio de un abogado, lo que conlleva el pago de sus respectivos honorarios, además, de los gastos procesales de búsquedas, notificación y tramitación en general. De modo que el procedimiento resulta tan extenso e innecesariamente costoso que la enorme mayoría de las personas no están dispuestas a tal desgaste por una situación 'de tan poca entidad' como la protección de un conjunto de datos personales.

Así, esta innovadora alternativa de defensa de la privacidad cayó en el olvido habiendo tenido muy pocas aplicaciones en sus más de 20 años de existencia. Es más, una importante fracción de los casos en que se intentó accionar por medio del *Habeas Data* fracasó por intentar proteger precisamente los datos personales que esta ley calificó como 'públicos', a saber, los antecedentes comerciales y financieros.

Finalmente, para aquellos casos en que la manipulación de los datos personales supuso una afectación de magnitud para su respectivo titular, se adoptó una práctica procesal que, pese a no estar contemplada de manera explícita en nuestro ordenamiento jurídico, logró construirse y validarse jurisprudencialmente como el mecanismo más adecuado para abordar las situaciones de uso ilegítimo de la información personal, esto es, el ejercicio de la Acción de Protección en virtud del artículo 19 n°4 de la Constitución Política de la República que asegura a todas las personas "El respeto y protección a la vida privada y a la honra de la persona y su familia". Para ello basta subsumir el caso a una hipótesis de afectación ilegal o arbitraria de la honra o privacidad del titular o su familia, haciendo posible ejercer una acción judicial que, de por sí, no supone gastos monetarios de consideración y que, además, puede llegar a término en semanas o al cabo de pocos meses.

En esta línea, y como una suerte de reafirmación tácita de la caducidad del *Habeas Data* como lo conocemos, en junio de 2018 una reforma constitucional extendió la protección del numeral 4° del art. 19 de nuestra Constitución a los datos personales, con lo que pasamos a reconocer de manera explícita el derecho fundamental a la autodeterminación informativa.

La presentación de este escenario regulatorio es relevante para efectos del Big Data toda vez que cualquier procesamiento masivo de información tiene como base el concepto de tratamiento a menor escala. Para que un sistema de tratamiento de datos masivos funcione conforme a derecho, es necesario

que cada uno de los millones de datos que son procesados y cada uno de usos sean obtenidos y empleados de acuerdo a los parámetros de la norma en cada etapa.

No obstante, es imposible garantizar el cumplimiento de estos estándares debido a las desmesuradas falencias de la regulación.

Un esquema normativo aplicable y efectivo requiere de 3 elementos: La norma, la sanción derivada del incumplimiento y el organismo encargado de fiscalizar y aplicar dicha sanción. Pues bien, en Chile sólo contamos con la norma. Aunque existen numerosas prácticas prohibidas por esta legislación, si se incurre en alguna de ellas, vulnerando la norma, no se derivan consecuencias adversas para el agente infractor, puesto que no hay un catálogo de castigos ni una entidad a cargo de la aplicación de la pena, lo que en la práctica constituye un incentivo descomunal para abusar de los datos personales de manera indiscriminada, generando con ellos enormes fuentes de riqueza y experimentando con toda índole de información sin consideración alguna respecto del impacto que de ello puede derivar para sus titulares, quienes quedan en una indefensión absoluta frente a las grandes compañías que transgreden sostenidamente los derechos que la ley les reconoce, negándose a su vez a dar cuenta de las actividades que llevan a cabo a costa de la privacidad de las personas.

Por último, vale la pena destacar que la ley 19.628 se redactó bajo la lógica del tratamiento que se podía dar a cada dato por separado y no pensando en los inmensos volúmenes de información y los diversos, veloces y exhaustivos mecanismos de procesamiento con que pueden ser analizados en la actualidad. Así, no hay disposiciones que contemplen la hipótesis del tratamiento de datos masivos ni sus consecuencias, con la sola excepción del artículo 5° de la ley que, sin haber sido pensado para estos efectos, tiene una aplicación extrapolable al caso:

> *Artículo 5°: El responsable del registro o banco de datos personales podrá establecer un procedimiento* ***automatizado*** *de transmisión, siempre que se cautelen los derechos de los titulares y la transmisión guarde relación con las tareas y finalidades de los organismos participantes.*
>
> *Frente a un requerimiento de datos personales mediante una red electrónica, deberá dejarse constancia de:*
>
> *a) La individualización del requirente;*
> *b) El motivo y el propósito del requerimiento, y*
> *c) El tipo de datos que se transmiten.*
>
> *La admisibilidad del requerimiento será evaluada por el responsable del banco de datos que lo recibe, pero la responsabilidad por dicha petición será de quien la haga.*

El receptor sólo puede utilizar los datos personales para los fines que motivaron la transmisión.

No se aplicará este artículo cuando se trate de datos sensibles accesibles al público general.

Esta disposición tampoco es aplicable cuando se transmiten datos personales a organizaciones internacionales en cumplimiento de lo dispuesto en los tratados y convenios internacionales.

De tal manera, la ley 19.628 se adelantaba al señalar algunos de los parámetros que hoy entendemos como aceptables para el tratamiento masivo de datos. Aquí, bajo la idea de normar el traspaso automatizado de bases de datos, no de datos individualmente considerados, la ley explicitó una serie de requisitos que sintonizan incluso con el RGPD, tales como que dicho traspaso tenga relación con las tareas y fines de los organismos participantes, que se individualice al requirente, que se manifieste cuál es el motivo y propósito (finalidad) del traspaso, que se especifique el tipo de datos que se están traspasando. Por si aquello no fuera suficiente, esta disposición también se encarga de generar un pequeño estatuto de responsabilidad para los participantes de la transacción obligando a quien maneja la base de datos a evaluar la pertinencia de la solicitud de información, pero manteniendo como responsable de la petición a quien solicitó los datos. Además, establece que quien reciba información producto de esta operación, sólo podrá utilizarlos para los fines explicitados en la transacción (principio de finalidad).

Con esta norma tan exhaustiva para su tiempo, teníamos un claro adelanto de la regulación de los participantes del tratamiento de datos personales que anticipaba la lógica regulatoria aplicable a lo que hoy conocemos como "tratamiento por encargo", cuyas notorias falencias en nuestra legislación pretenden ser subsanadas hoy por el proyecto de ley que se encuentra en tramitación.

Como ya se señaló, esta ley ha tenido una aplicación nimia y ha sido referenciada principalmente durante los últimos años por el mundo académico para evidenciar sus defectos, acusar su caducidad y visibilizar el enorme espacio de desregulación que se ha generado al alero del desarrollo de las tecnologías de la información.

c) Proyecto de Ley que modifica la Ley de Protección de la Vida Privada:

El 15 de marzo de 2017 la Presidenta Michell Bachelet ingresó al Senado el Mensaje N°001-365 con que se dio inicio a la tramitación del Boletín N°11144-07, proyecto de ley destinado a modificar la ley 19.628 y actualizarla para cumplir con los estándares que, por entonces, estaba imponiendo la UE con la reciente aprobación del RGPD.

En dicho Mensaje se podía leer el llamado que hacía la Primera Mandataria al Congreso en orden a observar los efectos de vivir en un mundo interconectado y cada vez más tecnologizado. Entre estos efectos se podían encontrar numerosas situaciones de la vida de las personas y de las relaciones entre privados que ya entonces ocurrían con habitualidad. Se enfatizaba el rol que jugaba la economía digital analizada en términos amplios, es decir, desde las transformaciones sociales, culturales y tecnológicas que convertían la economía actual en un entramado de relaciones muy diverso al que acostumbrábamos, toda vez que la sociedad digital había permitido la expansión de "los espacios de libertad, autonomía y desarrollo de las personas, pero también [había] diseñado nuevos y sofisticados sistemas de control y vigilancia que [amenazaban] o [limitaban] esa misma libertad" (Bachelet, 2017).

Este análisis de contexto consideraba también las implicancias del desarrollo de un sistema económico globalizado en que todos los países participan de un entorno financiero común y se interrelacionan en sus distintas transacciones, generando un modelo de economía que requería de la adaptación de sus regulaciones, prácticas e instituciones al uso generalizado de las tecnologías de la información. Para responder adecuadamente a este nuevo escenario, decía el Mensaje, el proyecto de ley recoge las recomendaciones efectuadas por la OCDE a sus países miembros, entre las que destacan materias relativas a la protección de la privacidad, al flujo transfronterizo de datos personales y a la necesidad de contar con una autoridad de control (Bachelet, 2017).

Al momento de escribir estas líneas, el proyecto fue aprobado por el Senado y remitido a la Cámara de Diputados, que actuará como Cámara revisora, por lo que de momento se encuentra en la Comisión de Constitución, donde se ha dado suma urgencia a su tramitación.

Aunque ciertamente la tramitación de este proyecto tuvo un avance considerable durante 2019, el estallido social de octubre y posteriormente la pandemia global llevaron al Congreso a un cambio en las prioridades legislativas, pasando a tomar protagonismo materias relativas a derechos sociales, salud, la tipificación de nuevos delitos asociados a las manifestaciones y los intentos por dotar de mayores atribuciones a Carabineros y Fuerzas Armadas.

Con todo, estos mismos escenarios han contribuido a evidenciar que sigue siendo urgente llegar a término en la tramitación de esta norma para contar con una regulación adecuada de la privacidad y los datos de las personas, toda vez que, en un contexto de convulsión social y/o de riesgo sanitario se corre el riesgo de que el Estado y sus agentes extralimiten sus facultades a la hora de perseguir y monitorear focos de disidencia que puedan ejercer derechos legítimos como los de reunión y manifestación. Por otro lado, en un contexto de crisis sanitaria como el actual, son recurrentes las propuestas orientadas a dar mayor difusión de datos sensibles, como los de salud, para facilitar las modelaciones y proyecciones de contagio, evolución y movilidad, e incluso para prevenir a los vecinos de un eventual foco de contagio

en su comunidad; asimismo, aparecen iniciativas de trazabilidad que en ocasiones apuntan a la obtención de tantos datos como sea posible, excediendo así su finalidad primaria, o que, estando bien intencionadas, no dan garantías adecuadas para proteger la delicada información que obtienen.

Así, resulta cada vez más claro que, en un mundo que funciona en base al tratamiento masivo de datos, contar con una regulación adecuada se vuelve crucial cuando se generan estados de crisis que requieren dar respuestas veloces y eficaces.

El actual grado de avance del proyecto de ley y el nivel de acuerdo que a estas alturas existe respecto de la mayor parte de su contenido, permiten presumir razonablemente que el texto no debiera seguir experimentando cambios significativos.

Teniendo esto como premisa, se expondrán los cambios que importará este proyecto de ley a la regulación del Big Data en el mediano plazo. Para ello, la primera pregunta a responder es cuál es el objeto de la norma.

Como cualquier herramienta o tecnología, el Big Data, o los programas y soportes necesarios para su aplicación, tienen un carácter neutro. Su utilización puede ser tremendamente útil para el desarrollo de investigaciones y puede implicar grandes avances en la organización de las sociedades, como también puede acarrear importantes riesgos para las personas y para segmentos sociales determinados. Es por ello que cuando hablamos de regular el Big Data, de inmediato caemos en una imprecisión y es que no se regula en sí el tratamiento masivo de datos, sino aquellos usos y ámbitos que revisten una mayor sensibilidad a la hora de trabajar con información.

De tal manera, lo que hasta ahora se ha regulado, y que constituye también el objeto de esta ley, es el tratamiento de los datos personales, incluyendo los aspectos específicos de su tratamiento masivo.

Esto implica que quedan fuera de la norma numerosas esferas que también son afectadas por la implementación de este tipo de tecnologías, pero que no se relacionan en forma directa con la privacidad de las personas. Algunas de estas esferas se revisarán en el capítulo IV de este trabajo para evidenciar el enorme entramado de relaciones que, por lo pronto, escapan a las normas.

Dicho esto, los principales aportes de la ley de protección de datos cuya aprobación se espera serían:

i) Creación de una autoridad de control.
ii) Consagración del interés legítimo como condición habilitante para el tratamiento de los datos personales y para justificar los segundos usos de esta información.

iii) Establecimiento del derecho a la portabilidad de los datos personales y sus limitaciones.

iv) Adición del derecho a la Impugnación.

v) Regulación explícita y pormenorizada del tratamiento masivo de datos personales.

vi) Determinación de los requisitos necesarios para dar segundos usos a la información: Establecimiento de las bases de licitud y la garantía de que los usos tengan una finalidad compatible con la autorizada originalmente.

La sola creación de una autoridad de control supone un cambio radical al actual escenario regulatorio, toda vez que materializa la posibilidad de fiscalizar y sancionar las conductas lesivas o abusivas que se dan en el tratamiento de datos personales, lo que, hasta el día de hoy sólo conlleva un reproche formal establecido en el texto de una ley que no cuenta con mecanismos efectivos de sanción.

Durante la tramitación del proyecto se debatió latamente si debía crearse un organismo de control nuevo y especializado o si debían entregarse estas atribuciones a una institución ya existente, y aunque, primordialmente por razones presupuestarias y de experiencia previa, en principio se había determinado que la institución encargada sería el Consejo para la Transparencia, en enero de 2022 el Senado despachó el proyecto habiendo optado por la creación de una agencia de protección de datos personales autónoma.

Para abordar los demás aspectos que incorpora este proyecto podemos subdividir la nueva regulación del Big Data en dos grandes categorías: En primer lugar, los requisitos que se deben cumplir para poder tratar datos masivos y, en segundo lugar, las exigencias que se impondrán a la actividad de tratamiento de datos masivos propiamente tal.

i) <u>Requisitos para tratar datos masivos:</u>

- **Finalidad Compatible:** Desde el momento de la obtención de la información debe existir un propósito que defina el por qué de la recolección. Dicho propósito o finalidad es el que delimita para qué pueden ser utilizados los datos, siendo ilegítima cualquier forma de tratamiento que transgreda este marco fijado ex ante, exceptuando los casos en que la información se obtiene de fuentes de acceso público.

  De tal manera, los datos deben obtenerse con fines específicos, explícitos y lícitos que, además, sean conocidos y autorizados por su titular; luego, el tratamiento de estos datos debe limitarse únicamente al cumplimiento de tales fines, no pudiendo extenderse a otros no considerados en un comienzo.

Este requisito generalmente se cumple mediante la publicación de políticas de privacidad que se encuentren a disposición de los usuarios.

No obstante, una de las novedades de esta norma es que incorporará la posibilidad excepcional de autorizar los segundos usos de la información personal previamente recolectada siempre y cuando se cumpla alguna de las siguientes hipótesis:

- **Que lo datos sean procesados sólo para fines compatibles con los autorizados originalmente**;
- Que entre el responsable de los datos y su titular exista una relación contractual o precontractual capaz de justificar el tratamiento de la información personal con fines distintos de los acordados, siempre que esta forma de procesamiento sea subsumible a los objetivos del contrato o relación precontractual;
- Que se otorgue un nuevo consentimiento;
- Que los datos provengan de fuentes de acceso público;
- Que así lo disponga la ley.

El Grupo de Trabajo del Consejo Europeo a cargo de este punto sostuvo que para poder hablar de finalidad compatible es necesario que dicha finalidad, aunque diferente, tenga relación con el propósito principal. Asimismo, se admite un cambio en el alcance o enfoque cuando las expectativas sociales o de los mismos titulares de los datos hayan variado respecto de los usos adicionales permisibles. Pero, en cualquier caso, es necesario que en un comienzo se haya determinado un propósito con el cual comparar el segundo uso que se pretende dar a la información (WP 203, 2013).

De tal manera, quedaría en manos de la nueva autoridad de control el determinar para los casos conflictivos si los fines aducidos por el responsable son efectivamente compatibles con los primarios atendiendo a criterios como la posibilidad de deducirse de cómo se expresan los fines originales, la naturaleza de los datos en cuestión, el grado de predictibilidad de la nueva operación, las medidas de seguridad, entre otros.

- **Mantenimiento de sistemas de seguridad acordes al tratamiento:**

  Un aspecto que ha demostrado ser de suma relevancia para efectos del tratamiento de datos personales corresponde al aseguramiento de la información. Quien se beneficia de determinados usos de la información tiene el deber de garantizar que los titulares de la misma no se verán expuestos por este hecho y que, en todo momento, sea protegido su derecho a la privacidad. Con este objetivo, las normativas contemporáneas de protección

de datos abordan la perspectiva de la seguridad de la información entregando parámetros a seguir por el responsable de los datos que, en todo caso, han de ser profundizados y fiscalizados por la autoridad de control.

Dado que ha sido la tónica de este proceso legislativo, para desarrollar este esquema se ha tomado como referencia el modelo de seguridad establecido por la UE, de modo que destacan aspectos como la Accountability o Responsabilidad Proactiva, la necesidad de elaborar Evaluaciones de Impacto para realizar determinados proyectos, el aseguramiento de la transparencia, información y garantía del cumplimiento de los derechos de los titulares. Además, la UE ha apostado por la incorporación de la privacidad desde el diseño y por defecto, es decir, apostar por que todo aquel que diseñe un mecanismo de procesamiento de información tenga en cuenta desde el inicio el deber de proteger la privacidad de los titulares de los datos y el respeto de la normativa vigente, de modo que el sistema por completo sea construido en base al cuidado de esta garantía y, por tanto, sea capaz de anticiparse a los riesgos inherentes del tratamiento de esta información.

La responsabilidad proactiva apunta a que las entidades que tratan datos personales asuman como propia la preocupación por su cuidado, para lo cual pueden tomar medidas como el establecimiento de protocolos internos que prevengan las infracciones, invertir en la capacitación de su personal en materia de datos, generar mecanismos de respuesta tanto para quejas como para fallas o ataques al sistema, la redacción de Códigos de Conducta vinculantes que den cuenta de su compromiso respecto de los métodos de tratamiento de datos y el establecimiento de canales de comunicación con los titulares que faciliten la entrega de información, la recepción de quejas y solicitudes (la entidad debe responder dentro de 15 días hábiles pudiendo efectuarse una reclamación ante la autoridad de control en caso contrario), la obtención del consentimiento cuando se requiera y el ejercicio de sus derechos.

Una de las herramientas útiles de las nuevas normativas de tratamiento de datos corresponde a las Evaluaciones de Impacto destinadas a evaluar el carácter y magnitud de los efectos que se pueden derivar de determinadas prácticas y usos de la información. Lamentablemente, este mecanismo, que fue establecido en el Reglamento Europeo, no ha sido incorporado hasta ahora en el proyecto de ley que se está tramitando en nuestro país. Sin perjuicio de ello, la facultad relativamente amplia que se otorga a la autoridad de control para generar mecanismos de cumplimiento y seguridad podrían abrir la posibilidad de requerir Evaluaciones de Impacto para llevar a cabo determinadas prácticas o proyecto. En esta misma línea, toman relevancia las auditorías aplicables al tratamiento de datos personales.

Así, con el objeto de mantener un adecuado control sobre las prácticas ejercidas sobre los datos y sus respectivos sistemas de información, existen numerosos procedimientos que debieran comenzar a desarrollarse en forma permanente, puesto que configuran mejoras cualitativas a los sistemas de seguridad de los datos y protección de la privacidad. Entre ellos destacan la anonimización, el cifrado, la trazabilidad, los controles de acceso para empleados, el desarrollo periódico de auditorías y la capacitación constante del personal involucrado en el tratamiento de datos.

La Anonimización es una técnica utilizada para disociar completa e irreversiblemente los datos personales de su titular a fin de evitar los riesgos que podrían derivarse de su reidentificación; en otras palabras, una correcta aplicación de este método debe eliminar toda posibilidad de identificar a una persona específica a partir del conjunto de datos que se tienen sobre ella. Para ello, y dado que no es posible obtener un resultado absoluto que vuelva inviable cualquier ejercicio de ingeniería inversa, lo que se debe intentar es conseguir un resultado cuya reversibilidad tenga un costo tan desproporcionadamente alto que no pueda ser abordado convenientemente en términos de esfuerzo-beneficio.

La secuencia de operaciones necesarias para la ocultación de la identidad de la persona ha recibido el nombre de "cadena de anonimización" y puede requerir, entre otros, de una evaluación de los riesgos asociados a la reidentificación de los titulares; el establecimiento de una escala de sensibilidad de la información que se tiene para poder clasificarla y referenciarla cualitativa y cuantitativamente; otro de sus aspectos característicos corresponde a la distorsión intencionada y controlada de los datos, donde lo que se busca es modificar levemente los antecedentes de cada titular – como al cambiar la edad u origen geográfico-, pero sin alterar el resultado final de la medición de dichos datos, de modo tal que el conjunto mantenga su funcionalidad inicial, siendo aconsejable el diseño de un protocolo para el equipo a cargo del proceso (Agencia Española de Protección de Datos, 2016).

El Cifrado de la información o Encriptación corresponde a una operación reversible que transforma el conjunto de datos significativo en datos ilegibles que solamente pueden ser descifrados mediante el uso de una clave cuya utilización los vuelve nuevamente legibles. Así, la finalidad de esta operación es que el contenido del mensaje sólo pueda ser conocido por su destinatario.

En la actualidad, ha comenzado a utilizarse ampliamente el cifrado de punto a punto, mecanismo de seguridad que consta de dos etapas: El primer paso de la comunicación es la posibilidad de conocer una determinada dirección, generalmente de conocimiento público, a la que enviar un mensaje; el segundo paso es la posibilidad de que el receptor pueda leer y comprender el mensaje que recibió, para lo cual debe estar en posesión de una clave única y personal que decodifique el mensaje. El sistema es sumamente efectivo, ya que cada dispositivo tiene su propia clave, motivo por el que una conversación

entre dos dispositivos sólo puede ser comprendida por ellos dos, y si existe un tercero que logra interceptar el mensaje y hacerse del texto, lo único que podrá visualizar son caracteres y símbolos que no reportan sentido alguno para el lector (Bauzá, 2017).

Este mecanismo de seguridad ha sido adoptado por varias compañías que requieren de vías confiables para transmitir su información crítica, así como también por importantes empresas de mensajería instantánea entre las que destacan Whatsapp, Telegram y Signal.

Por otro lado, la Trazabilidad de los datos corresponde a un proceso de registro de la información y sus etapas, que entrega la posibilidad de localizar un dato determinado en cualquier punto de la cadena de tratamiento, lo que resulta fundamental a la hora de garantizar los derechos de sus titulares y también a la hora de dar cuenta de la legalidad de todas las operaciones que se llevan a cabo sobre la información. Mantener un sistema de seguimiento como este, que permita vislumbrar de manera íntegra las etapas del proceso junto con toda la información que se encuentra circulando en él, constituye un presupuesto de suma relevancia para poder desarrollar auditorías sobre los mecanismos de tratamiento de los datos y la protección de los derechos de sus titulares.

Como ya se indicaba, el éxito de la implementación de medidas de seguridad como las aquí descritas requiere de un trabajo permanente de monitorización de los sistemas y los datos, de la realización de auditorías, del establecimiento de protocolos de acceso que discriminen qué empleados pueden visualizar y/o utilizar las bases de datos y sus sistemas de procesamiento y también de la profesionalización de quienes desempeñan roles asociados al tratamiento de la información.

- **Establecimiento de estándares de cumplimiento acordes a las características de la entidad:**

  Los elementos revisados en el punto anterior configuran el esquema de protección que el proyecto de ley de protección de datos personales establece como estándar adecuado de cuidado. Sin perjuicio de ello, el legislador tuvo en consideración la dificultad que importa la realización de dichas conductas para gran parte de las empresas y organizaciones que componen el mundo privado y que también requieren del tratamiento de datos personales para el desarrollo de su respectiva función. En atención a ello, el proyecto contempla la posibilidad de aplicar estándares diferenciados de cumplimiento respecto de los niveles de seguridad atendiendo a criterios como el volumen de datos procesados, el tamaño de la empresa o corporación y al hecho de tratarse o no de una persona jurídica.

En todo caso, la fijación y especificación de estos estándares será una de las tareas que deberá desarrollar la futura autoridad de control.

ii) Exigencias para el desarrollo de la actividad de tratamiento de datos personales:

Una vez que se cumple con los requisitos previos y se instala un modelo de tratamiento seguro y respetuoso de los derechos de los titulares, pasa a ser necesaria la obtención de la información y su correspondiente procesamiento.

Recordemos que, a diferencia de la normativa vigente, el proyecto de ley sí se hace cargo de regular el tratamiento masivo de datos. Para ello, el artículo 15 ter señala que "El responsable de datos podrá establecer procedimientos automatizados de tratamiento y transferencia de grandes volúmenes de datos, siempre que los mismos cautelen los derechos del titular y el tratamiento guarde relación con las finalidades autorizadas por los titulares".

Aunque todavía no se ha zanjado la discusión sobre incorporar explícitamente al artículo 15 ter la remisión a los requisitos para el tratamiento masivo de datos contenidos en los artículos 12, 13 y 8 bis del mismo proyecto, es importante referirlos ya que contar con alguna de las bases de licitud de los artículos 12 y 13 constituye un requisito fundamental para cualquier tratamiento de datos personales, mientras que el derecho de los titulares para oponerse a las decisiones perjudiciales que sean tomadas en su contra basadas únicamente en el tratamiento de un algoritmo pasará a ser una garantía inherente al tratamiento masivo de datos una vez que este proyecto se convierta en ley.

En otras palabras, los requisitos copulativos que exigirá la ley para el tratamiento masivo de datos personales serán los siguientes:

- **Cautela de los derechos de los titulares:** Hasta ahora, los derechos que conoce nuestra legislación son los denominados derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) y el derecho a Bloqueo de los datos que, según la propia ley 19.628 son indisponibles, no pudiendo ser limitados por convención alguna a excepción de disposiciones legales, razones de seguridad nacional o de interés público.

  Pero existe una garantía adicional que consiste en el aseguramiento del ejercicio o exigencia de estos derechos, a saber, la acción de *Habeas Data* que, como vimos, es el mecanismo mediante el cual todos los titulares de datos personales pueden hacer valer estos derechos cuando estimen que han sido vulnerados, o bien, exigir una rendición de

cuentas respecto de la manera en que se está llevando a cabo el procesamiento de su información.

Con todo, el proyecto de ley pretende extender el actual catálogo de derechos incorporando dos nuevas garantías: el derecho a la Portabilidad y el derecho a la Impugnación, de modo que la conocida sigla nemotécnica pasaría a ser la de los derechos ARCOPI.

Para comprender mejor manera lo que implica cada uno de los derechos ARCOPI, los desarrollaremos a continuación distinguiendo su configuración actual y los elementos que le aporta a cada uno el proyecto de ley.

- Derecho de Acceso: Permite al titular conocer los datos que sobre él tiene cualquier entidad, pudiendo requerir toda información relativa a sus datos, tal como el modo y fuente en que se obtuvo, su destino, el propósito de su almacenamiento y la identidad de las personas u organismos a los que serán transmitidos.

  El proyecto refuerza este derecho al agregar algunas hipótesis de uso al catálogo de posibilidades entregado por la ley 19.628. Estas hipótesis son la posibilidad de pedir que el responsable de la información confirme si sus datos, y cuáles datos, están siendo tratados por la entidad, pudiendo exigir el acceso a los mismos, a su origen, finalidad, categorías, tipos de destinatario y la identidad de estos.

  Ciertamente, esta nueva forma de exponer las alternativas provistas por el derecho de acceso no modifica el universo de posibilidades a que da lugar su versión actual, siendo sólo relevantes su reafirmarción y la certeza de que, a diferencia de lo que ocurre hoy, una vez aprobado este proyecto, sí existan instancias y garantías para el ejercicio de este derecho.

- Derecho de Rectificación: Faculta al titular para solicitar al responsable que modifique o rectifique sus datos cuando sean inexactos, estén desactualizados o incompletos. Es más, de acuerdo con este derecho, el responsable del tratamiento tiene el deber de corregir, actualizar o complementar la información cuando tenga conocimiento de datos que ya hubieran sido rectificados, incluso si el titular no ha solicitado el ejercicio de este derecho.

  A pesar de que el proyecto de ley mantiene este derecho, elimina la obligación del responsable de rectificar los datos cuando no medie una solicitud del titular y, junto con ello, agrega la obligación de que los datos que fueren rectificados deberán ser comunicados a las entidades a las que dicha información hubiera sido cedida o

comunicada con antelación por parte de la institución requerida, no pudiendo estas volver a utilizar la versión anterior de tales datos.

- Derecho de Cancelación: Este derecho es el que, ya en la actualidad, habilita al titular para requerir al encargado la eliminación de su información cuando su almacenamiento carece de justificación legal o cuando los datos han caducado. Tal como ocurre con la rectificación, no es necesario que el titular requiera esta acción para que el encargado de los datos la ejecute, dado que este tiene el deber de cancelar dicha información cuando se percate de la procedencia de dicha medida. Al igual que con el derecho de rectificación, el proyecto de ley pretende suprimir esta obligación del responsable en los casos en no media una solicitud del titular. Con todo, el proyecto también se encarga de agregar otros supuestos bajo los cuales procede el ejercicio de este derecho que, hasta ahora, se halla limitado a sólo 2 causales de concurrencia. Estos nuevos supuestos contemplan aquellos casos en que los datos no digan relación con los fines del tratamiento, cuando se haya revocado el consentimiento del titular no existiendo otro fundamento legal para su conservación, cuando los datos se hubieren obtenido de manera ilícita, cuando hubieren caducado, cuando fuera necesaria su supresión para dar cumplimiento a una sentencia judicial u otra obligación legal y también cuando el titular ejerciere su derecho a oposición. Sin perjuicio de ello, el nuevo texto precisa que este derecho podrá ser desplazado cuando la información en cuestión sea necesaria para el ejercicio de las libertades de opinar e informar, cuando se requiera para la ejecución de una obligación legal o de un contrato, en aquellos casos en que existan razones de interés público, cuando el tratamiento tenga fines históricos, estadísticos, científicos o de estudios que apunten al interés público y en los casos en que se verifique la formulación de una reclamación administrativa o judicial.
- Derecho de Oposición: Consiste en la facultad del titular para exigir que sus datos personales no sean tratados con fines de comunicación comercial, lo que le permite ser eliminado del registro respectivo. Este derecho no debe confundirse con el derecho de cancelación, toda vez que responden a hipótesis distintas sin perjuicio de poder llegar a concurrir de manera conjunta.

  El derecho de oposición es, probablemente, una de las garantías más evidente y reiteradamente vulneradas de la ley 19.628, pues es de público conocimiento la molestia que generan los spams publicitarios y las llamadas desde agencias de *call center* para ofrecer productos y servicios que, la gran mayoría de las veces, nadie ha

solicitado. Peor aun, resulta habitual el reclamo de quienes solicitan al ejecutivo telefónico que borre la información de sus registros, hallando como respuesta que los ejecutivos no están facultados para eliminar los datos, o bien la finalización de la comunicación.

Al igual que en el caso anterior, el proyecto de ley que modifica la ley 19.628 amplía los márgenes de aplicación de este derecho al incorporar nuevos supuestos para su ejercicio, a saber, aquellas situaciones en que el tratamiento de la información conlleva una afectación para los derechos y libertades fundamentales del titular y también cuando los datos tratados se hayan obtenido de una fuente de acceso público y no exista otro fundamento legal para su conservación, manteniéndose además las situaciones en que el tratamiento o uso de los datos responde a fines exclusivamente publicitarios o de marketing directo. No obstante, este texto también establece supuestos de excepción en los que el responsable del tratamiento podrá eximirse del cumplimiento de este derecho cuando la utilización de los datos resulte necesaria para resguardas las libertades de opinar e informar, cuando existan razones de interés público para su utilización, cuando el tratamiento tenga fines históricos, estadísticos, científicos o estudios que atiendan a fines de interés público y cuando se requieran para la formulación de una reclamación administrativa o judicial.

- Derecho a Bloqueo: A diferencia de los derechos anteriores, el de bloqueo tiene como característica propia la provisoriedad de sus efectos, pues se trata de una suspensión temporal del uso o tratamiento de los datos personales concretos que, para efectos de su procesamiento, quedan congelados mientras dura el supuesto que da lugar a su ejercicio. Estos supuestos corresponden a las situaciones en que se genera duda acerca de la calidad del dato, de su veracidad o exactitud; también procede cuando se configura una disputa entre el titular y el responsable respecto de las circunstancias de su tratamiento, debiéndose esperar una resolución del conflicto antes de decidir si el dato debe desbloquearse, modificarse o, en definitiva, eliminarse. Igualmente, el titular puede ejercer su derecho a bloqueo cuando existan motivos de confidencialidad, pero en estos casos lo que se hace es evitar la publicidad del dato, mas no su tratamiento por parte del responsable, quien debe limitarse a tomar las medidas necesarias para que dicha información no pueda ser conocida por terceros. Otra hipótesis, contemplada tanto en la ley 19.628 como en el proyecto, es la suspensión del tratamiento en beneficio del titular, como ocurre,

por ejemplo, cuando el dato de morosidad generado durante un período de cesantía de un deudor le importe perjuicios actuales.

Uno de los aspectos más característicos de este derecho es su complementariedad, toda vez que puede ejercerse fundadamente junto con las solicitudes de rectificación, cancelación u oposición con el objeto de lograr el bloqueo del tratamiento de los datos en disputa mientras dura la controversia principal. De conformidad con el proyecto, todas las controversias suscitadas a este efecto deberán ser revisadas por la autoridad de control.

- Derecho de Impugnación: Este derecho es por completo una novedad del proyecto de ley que modifica la ley 19.628 y se encuentra en su artículo 8° bis. Probablemente su único precedente dentro de nuestra legislación se pueda encontraren el artículo 5 de la actual normativa que, como revisábamos al comienzo de este capítulo, es la única disposición de nuestra ley que contempla el tratamiento automatizado de los datos personales. Pues bien, el derecho de impugnación consagra la posibilidad de que el titular se oponga a una decisión automatizada que le afecte significativamente cuando este resultado haya sido obtenido únicamente a partir de sistemas automatizados de procesamiento de información. De tal manera, los resultados de los mecanismos de análisis basados en inteligencia artificial, los sistemas predictivos o de análisis pueden ser objetados en sus conclusiones por el titular de la información que procesan, pudiendo refutarlos y exigir al responsable que dé cuenta acerca de los factores que llevaron al sistema a la toma de tal decisión. Así, el escenario por antonomasia para el ejercicio de este derecho corresponde al tratamiento automatizado de grandes volúmenes de datos y su gran particularidad es que asegura a todas las personas la posibilidad de que intervenga un ser humano en la toma de una decisión que pueda tener repercusiones sobre el titular. Aun así, pueden exceptuarse de la protección de este derecho los casos en que la elaboración del análisis, perfil u otro deriven de un acuerdo contractual, la entrega del consentimiento o la disposición de la ley.
- Derecho de Portabilidad: Al igual que el derecho de impugnación, el derecho a la portabilidad de los datos personales pretende ser incorporado a nuestra legislación mediante la aprobación del proyecto de ley que modifica la ley 19.628. El objetivo de la portabilidad es otorgar a los titulares interesados la posibilidad de requerir el conjunto de datos personales que han proporcionado a un responsable de tratamiento sin la necesidad de justificar el motivo de dicho requerimiento. Una vez hecha esta

solicitud, el responsable del tratamiento tiene la obligación de entregar el conjunto de datos en un formato estructurado, de uso común y lectura mecánica interoperable, todo esto a fin de desarrollar en los interesados una mayor capacidad de control sobre su propia información.

Entre las consecuencias de una eventual cotidianeidad en la aplicación de este derecho, podría generarse un escenario de permanente flujo de información de un responsable a otro, pero que, a diferencia del modo en que ocurre en la actualidad, tendría que ser eliminada por el primero para llegar a manos del segundo.

El presupuesto de la aplicación del derecho a la portabilidad en Chile será el tratamiento automatizado de datos siempre que dicho tratamiento se justifique debido al consentimiento inequívoco del titular.

Es probable que este sea uno de los derechos que suscite más conflictos cuando el mentado proyecto de ley entre en vigencia, puesto que su ejercicio conlleva como presupuesto la determinación de cuál es la información que la entidad debe entregar obligatoriamente al titular y cuál no. Esto es problemático dado que las empresas invierten para obtener datos personales, por lo que la existencia de una obligación legal de tener que entregar este activo a un tercero cuando el titular lo dispone puede entenderse como estar haciendo el trabajo de la competencia. Sin perjuicio de ello, el asunto resulta sensible toda vez que los sistemas de inteligencia artificial se entrenan y se vuelven más precisos en la medida que tienen acceso a mayores volúmenes y variedades de información, lo cual pone a cualquier entidad que se dedique al tratamiento de datos en la necesidad de buscar mecanismos e incentivos para conservar la información a la que tienen acceso, pudiendo llegar a desarrollar políticas de obstrucción a la portabilidad o de mantener la información en lugar de borrarla al momento de la entrega. De ahí que la trazabilidad y la capacidad de fiscalización de la autoridad de control se tornen tan relevantes.

En cualquier caso, cuando un titular ejerza su derecho a la portabilidad lo que se deberá analizar será qué datos corresponde entregar y cuáles puede conservar la entidad. Para ello el criterio de diferenciación estaría puesto en la circunstancia de haber sido facilitada la información de manera directa y consentida por el titular o de haber sido obtenida producto de un proceso de observación, análisis y conclusión por parte de la entidad. Esto bajo el entendido de que la información proporcionada por las personas es posteriormente tratada y de ella se extraen numerosas conclusiones que pueden apuntar a la creación de perfiles de los usuarios, al

conocimiento de determinados hábitos, a probabilidades sobre sus gustos y sus futuros movimientos, entre otras.

La información proporcionada por los titulares, también conocida como datos internos, es aquella que ha sido proporcionada de manera consentida por los titulares y puede consistir, por ejemplo, los datos de contacto o los que provienen de canales digitales como las redes sociales, páginas web, las plataformas de compra en línea, el uso de aplicaciones, etc. Sobre toda esta gama de datos se debe garantizar el derecho a la portabilidad, quedando fuera de su esfera de protección la información obtenida en base a la observación del comportamiento, como la que consigue a través de sistemas de monitoreo como los de biometría para identificación (reconocimiento facial, dactilar, de iris), los circuitos cerrados de cámaras de video y la identificación de las patentes de vehículos; también quedan fuera de la custodia de la portabilidad los datos externos adquiridos comercialmente de proveedores externos, empresas de sondeo, así como los deducidos o inferidos de un proceso de análisis.

Cabe destacar que, la mayor parte de las veces, esta información derivada de un proceso de análisis sobre el conjunto original corresponde más a una probabilidad que a un dato exacto, por lo que, en ocasiones, se ha puesto en duda su calidad de dato personal. Con todo, estos datos sí dicen relación con la persona que refieren y pueden predecir mucho sobre ella con un rango de error cada vez más bajo. De ahí que el asunto se vuelva tan delicado y llano a interpretaciones.

Aunque este criterio es el que seguramente se impondrá una vez aprobado el proyecto de ley, resulta necesario señalar que la distinción entre un dato personal y un dato probabilístico sobre una persona parece artificiosa a la hora de determinar regímenes de tratamiento diferenciados, en tanto se parte del supuesto de que todo "dato personal" es un dato duro y objetivo acerca del titular que refiere. No obstante, entre estos datos existen varios que corresponden a una mera aproximación o probabilidad, siendo el caso más sencillo de ilustrar el de los antecedentes médicos que, como ya vimos, corresponden a la categoría de dato personal sensible en vista de los significativos efectos que puede tener sobre la vida de una persona su difusión o aprovechamiento. Aun así, gran parte de los antecedentes médicos no son sino probabilidades del padecimiento de una enfermedad o del grado de predisposición a desarrollar otras patologías. Si bien existen diagnósticos bastante certeros, sabemos que lo que evalúan, por ejemplo, los sistemas privados de salud o las

compañías de seguros, son nuestros antecedentes médicos, los de nuestra familia y, muchas veces, los exámenes que nos hayamos realizado que pudieran evidenciar otros padecimientos; todo esto con el objeto de generar un perfil médico que dé cuenta de la probabilidad de desarrollar alguna patología que conlleve la necesidad de subir la prima asociada a salud a la hora de la contratación. En términos más sencillos, del hecho de que un familiar cercano haya padecido un cáncer, no se desprende necesariamente que una persona vaya a desarrollar uno, pero sí lo vuelve más probable, y resulta que el sólo hecho de ese aumento en la probabilidad puede derivar en un aumento de los costos de salud para la persona. Entendiendo esto, resulta sencillo dilucidar cómo el tratamiento y predicciones hechas por los sistemas de procesamiento de información pueden afectar las decisiones que las empresas toman respecto de sus afiliados actuales y potenciales. De manera que cobran una relevancia gravitante no sólo la información que se facilita, sino también la que se puede deducir y que, al no ser objeto de protección del derecho a la portabilidad, se aleja de la esfera de custodia de su titular, quien, en principio, no puede optar por traspasarla a una entidad distinta.

Sin perjuicio de lo anterior, del hecho de que sobre la información derivada no concurra el derecho a la portabilidad no se desprende que tampoco concurran los demás derechos (ARCOI), ya que, en la medida que entendamos que dicha información tiene un carácter personal, es decir, que refiere a una persona identificada o identificable, es posible solicitar los derecho de Acceso, Rectificación, Cancelación, Oposición e Impugnación sobre ella.

En cuanto a las sanciones por la vulneración de estos derechos, como vimos con anterioridad, contamos en la actualidad con la acción de *Habeas Data* del artículo 16 de la ley 19.628, que permite al titular reclamar, primero en forma directa y luego por vía judicial, para lograr el restablecimiento de sus derechos. No obstante, las condenas por este tipo de infracción son escasas y cuando se acompañan de una sanción monetaria, esta no apunta a la infracción en sí, sino que suele justificarse en el daño a la honra o al daño moral que pueda haber sufrido el afectado debido al tratamiento lesivo de los datos. Es difícil encontrar casos en que se aplique una sanción por la infracción de la norma dado que nadie fiscaliza el tratamiento de los datos y, como ya se explicó, los usuarios no parecen dispuestos a embarcarse en un juicio para reclamar sus datos personales.

Atendiendo a esta falencia, el proyecto contempla una escala de gravedad para las infracciones que se categorizarán en leves, graves y gravísimas, siendo este el criterio para determinar el rango monetario de la condena que será de 1 a 100 UTM, de 101 a 5000 UTM y de 5001 a 10.000 UTM, respectivamente para cada incumplimiento. Así, finalmente, se establecerán sanciones considerables que incentiven al cumplimiento de la ley.

Adicionalmente, se creará un Registro Nacional de Cumplimiento y Sanciones en que serán anotados quienes hayan sido sancionados por la comisión de infracciones graves y gravísimas, debiendo dejar constancia de la conducta infraccional, las agravantes y atenuantes respectivas, junto con la sanción impuesta. Los datos de este registro serían de acceso público durante 5 años desde practicada la anotación.

- **El tratamiento debe guardar relación con las finalidades de las personas o entidades participantes:** Este requisito para el tratamiento automatizado de datos personales es una particularidad de nuestro proyecto de ley, no pudiendo encontrarse en el RGPD ninguna norma equiparable. El objetivo de este requerimiento consiste en asegurar que el tratamiento que se lleve a cabo sobre un determinado conjunto de datos tenga relación con los fines, giro empresarial o función de la entidad responsable de dicho tratamiento, el cual, en caso de tratarse de una persona jurídica, debiera estar explicitado en su escritura de constitución. De esta manera se busca evitar que la entidad en cuestión pueda inventar cualquier finalidad a modo de pretexto para procesar una mayor variedad de información con fines diversos a los que le corresponde atender.
  Es más, cuando el tratamiento se realice de forma coordinada entre varias entidades, será necesario un acuerdo escrito entre estas donde la finalidad expuesta sea compatible con los giros o funciones de cada una de ellas.

- **Contar con alguna de las bases de licitud de los artículos 12 o 13:** Las bases de licitud o condiciones habilitantes para el tratamiento de datos personales, son las formas en que se ha denominado de manera genérica al listado de presupuestos bajo los cuales es lícito el tratamiento de los datos referidos a una persona. Estos requisitos no son copulativos, de modo que, para la mayor parte de los casos, basta la concurrencia de uno solo de estos presupuestos para que el interesado pueda procesar la información en cuestión. Las bases de licitud están tratadas en los artículos 12 y 13 del proyecto de ley, siendo el

artículo 12 el que desarrolla el consentimiento y el artículo 13 aquel que contiene todas las otras hipótesis u excepciones a la regla principal que dan lugar al tratamiento de los datos personales pese a no existir consentimiento del titular en los términos de la disposición anterior. Las condiciones habilitantes son la siguientes:

- Consentimiento: Hasta este punto se ha hablado bastante acerca del consentimiento, pero, pese a ser uno de los pilares del modelo de regulación del tratamiento de datos personales, no hemos desarrollado el concepto. El consentimiento, para estos efectos, corresponde a una manifestación de voluntad libre, específica, informada e inequívoca del titular que se expresa en un acto afirmativo en orden a aceptar el tratamiento de un conjunto determinado de sus datos personales. Se ha requerido en las distintas regulaciones de protección de datos que este consentimiento se exprese por escrito o, cuando menos, a través de un mecanismo que deje registro de la aceptación y que pueda, posteriormente, servir como un medio de prueba que lo acredite en forma inequívoca. Además, una vez conocida la o las finalidades del tratamiento, el consentimiento debe otorgarse para todas las operaciones destinadas a la obtención de dichos fines.

  Normalmente, para efectos de los contratos o políticas de privacidad que aceptamos en línea, suele bastar con nuestro click de aceptación de los términos para entender que hemos dado nuestro consentimiento expreso e inequívoco a su respecto. Así es como se ha entendido en Chile y en la mayor parte del mundo hasta ahora.

  Sin embargo, existen voces disidentes que apuntan a que no es posible entender un simple click como criterio verificador de un consentimiento voluntario respecto de términos y condiciones extensos y complejos para el usuario promedio, quien no tiende a leer tales condicionantes y acepta los términos sin mayor análisis para poder acceder a una prestación determinada (Bundeskartellamt, 2019).
- Datos recolectados de una fuente de acceso público: Aunque las fuentes de acceso público no se detallan en el RGPD, ni existe un catálogo taxativo en nuestra legislación actual ni tampoco en el proyecto en tramitación, lo que se pretende cuando se las menciona es referir aquellas bases de datos personales que, como su nombre lo indica, se encuentran puestas a disposición del público de manera que cualquiera puede conocer ese tipo de dato respecto de cualquier tercero que se encuentre contemplado en el conjunto de información. Esto ocurre en Chile con los antecedentes del Registro Civil, a saber, fecha de nacimiento, C.I., filiación, estado civil, antecedentes penales, el hecho de tener o no propiedad sobre vehículos

motorizados, entre otros; lo propio ocurre con la información comercial que se encuentra contenida y sistematizada por EQUIFAX, empresa a la que se pueden solicitar los antecedentes comerciales de cualquier persona a cambio de un pago. Así, lo que define a la fuente de acceso público no es que la disponibilidad de los datos sea gratuita o tenga asociado un costo, sino el hecho de que cualquier persona tenga la posibilidad de acceder libremente y sin expresión de causa a su contenido y que dicho acceso sea legítimo. Esta legitimidad significa que, hipotéticamente, si una persona interceptara un sistema de información y sustrajera datos que se encontraban protegidos para posteriormente darlos a conocer en una red social a través de una cuenta pública, dicha fuente no sería una fuente de acceso público, sino un espacio de divulgación ilegal de datos personales que no podría legitimar la utilización de estos por parte de los interesados que pudieren acceder a tales contenidos y que, además, convertiría al autor de la divulgación en acreedor de una de las sanciones contempladas en el proyecto y en la ley 19.223.

Con todo, es debatible el alcance que tienen estas fuentes. Mientras que, por un lado, Alberto Cerda sostiene que, para una interpretación armónica de la ley y su espíritu, debe entenderse que todas las bases de datos son restringidas a menos que exista una ley que declare lo contrario, por otro, Renato Jijena ha afirmado que al encontrarse concebidas por la legislación chilena las bases de datos reservadas, se entiende *a contrario sensu* que todas aquellas que no tengan tal categoría son de acceso público. Frente a esta disyuntiva, Francisco Alvarado Ávalos entrega una salida razonable al distinguir entre bases de datos cuyo responsable es un particular y aquellas cuyo responsable es un organismo público. En las primeras, al no existir una caracterización legal de unas y otras, determinar su naturaleza dependería de su responsable; en las segundas, habría que atenerse a los dispuesto por la ley 20.285 sobre acceso a la información pública para los casos en que la ley no señale si se trata de una fuente de acceso público o no. El artículo 21 de la ley 20.285 establece las causales que permiten discriminar cuándo corresponde que un organismo público deniegue a un interesado el acceso a determinada información. Entre estas causales se encuentran contemplados los casos en que la publicidad, comunicación o conocimiento de tales datos afecte los derechos de las personas, particularmente tratándose de su seguridad, salud, la esfera de su vida privada o derechos de carácter comercial o económico (Ávalos, 2014).

Dado que nuestra actual legislación no establece un catálogo de fuentes de acceso público, es muy fácil dar espacio a discusiones sobre si una determinada fuente es o no subsumible en esta definición. Así, los únicos casos respecto de los que existe una certeza absoluta corresponden a los enumerados en el artículo 4 de la ley 19.628 que establece que los datos que pueden formar parte de una fuente accesible al público son los de carácter económico, bancario, financiero o comercial, así como también los relativos a una categoría de persona en la medida que se limiten a señalar su pertenencia a un grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, y también los que sean necesarios para comunicaciones comerciales o venta directa de bienes o servicios (marketing directo). En contraposición con esto, el proyecto de ley no contempla ninguna enumeración explícita a las fuentes de acceso público, limitándose a indicar que este tipo de fuente existe y que constituye por sí misma una base de licitud.

Lograr determinar cuáles son estas fuentes es relevante toda vez que, para obtener, tratar e incluso ceder estos datos no resulta necesaria la obtención del consentimiento del titular ni cumplir con el deber de confidencialidad a su respecto.

- Tratamiento de datos relativos a obligaciones económicas, financieras, bancarias o comerciales: Esta excepción de la ley 19.628 se mantiene en el artículo 17 del proyecto que regula los casos en que puede tratarse la información financiera y comercial de las personas con el fin de resguardar la certeza tanto económica como jurídica respecto de la probabilidad de cumplimiento que existe en el marco de la celebración de un negocio con una persona determinada. Así, se busca proteger la libre circulación de los bienes y la credibilidad de los espacios de mercado.
- Tratamiento necesario para la ejecución o cumplimiento de una obligación legal o por disposición de la ley: Con esta excepción se efectúa una ponderación que, en abstracto, favorece el cumplimiento de la ley por sobre la protección de los datos que pudieran requerirse para estos efectos. Por supuesto, los datos que deban ser provistos para ello no pueden ser destinados a ninguna finalidad diversa al cumplimiento de la obligación legal que justifica su utilización.
- Tratamiento necesario para la celebración o ejecución de un contrato entre el titular y el responsable o para la ejecución de medidas precontractuales adoptadas a solicitud del titular: Al igual que en la excepción anterior, con esta base de licitud se pretende dotar de mayor seguridad a las relaciones jurídicas, especialmente entre privados, donde pueden concurrir engaños u ocultamientos entre las partes para

sacar provecho. Así, cuando una de las partes hubiere solicitado ciertas medidas precontractuales o firmado un contrato cuya ejecución requiriera del acceso a sus datos personales, en principio, estos debieran ser entregados para tales efectos.

- Interés Legítimo: Aunque existe controversia, hay quienes sostienen que es posible deducir que esta condición habilitante se encuentra contemplada en forma tácita en nuestra actual legislación sin perjuicio de que no se mencione en la enumeración de excepciones contenidas en la ley 19.628 que se encarga de señalar de manera explícita los casos en que se puede legitimar el tratamiento de datos personales pese a no contar con el consentimiento del titular. Sin embargo, quienes lo afirman parten de la base de que el artículo 4 de la ley 19.628 sostiene que el tratamiento de los datos debe responder a actividades en beneficio de "personas jurídicas privadas", lo que autorizaría a estas entidades a procesar los datos de los titulares aun sin su consentimiento siempre que lo hagan para uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros que les beneficien. Esta última restricción es importante ya que limita el ámbito de protección de esta habilitante únicamente a los usos de la información que se lleven a cabo al interior del grupo económico, no encontrándose facultados para ceder o difundir la información personal y, por cierto, siempre que los usos que se den a la información sean acordes a la ley, para fines permitidos por el ordenamiento jurídico y respetando el pleno ejercicio de los derechos y facultades de los titulares de la información.

  En cualquier caso, queda poco tiempo para insistir en esta disyuntiva habida cuenta de que el proyecto de ley pretende establecer de manera explícita esta condición habilitante para el tratamiento de datos personales al incorporarla en su artículo 13 letra e) como una de las "otras fuentes de licitud distintas al consentimiento". Ahora, ¿A quién corresponde este interés legítimo y en qué consiste? Esta base de licitud está pensada desde la perspectiva del responsable del tratamiento de datos, dado que, en la era de la informática, resulta de toda lógica que las empresas y organismos públicos requieran de una infinidad de datos para perfeccionar sus productos y servicios. Para lograrlo parece necesario otorgar una mayor gama de alternativas para potenciar y desarrollar esta actividad de un modo tal que no lesione los derechos de los particulares que acaban involucrados en el tratamiento.

  Cabe recordar que, para el derecho, el interés legítimo es un derecho que debe ser ejercido bajo la observancia de una justa ponderación de prioridades entre los

intereses que pueden llegar a confrontarse en el marco del tratamiento de los datos. Su fundamento se encuentra en la libertad fundamental que tenemos todos de desarrollar actividades económicas siempre que estas no vulneren los derechos de terceros. Así, para que este interés legítimo pueda jactarse de su legitimidad, es menester que cumpla con una serie de condiciones que, según ha entendido el legislador, lo convierten en un derecho que se puede ejercer en armonía con el ordenamiento jurídico, por lo que no basta con la mera existencia de una motivación de carácter económico o comercial para entender que se configura el interés legítimo.

En este sentido, el Grupo de Autoridades de Control de la Unión Europea ha sostenido que el interés legítimo se relaciona con el concepto de "finalidad", siendo esta última el motivo por el que los datos pueden ser tratados, mientras que el interés legítimo se correspondería con el beneficio que reporta para el responsable su utilización. De tal manera, la legitimación del interés no podría lograrse de la ponderación abstracta del interés del titular versus el interés del responsable, sino de un análisis concreto de cada situación (WP 203, 2013). Esto hace necesario que el responsable defina cuál es el objetivo o intención del tratamiento de los datos en cuestión. Los objetivos o intenciones que se determinen, evidentemente, deben ser aceptables desde una perspectiva legal – aquí se pueden tener en consideración elementos como el tipo de relación que tiene el responsable con el titular, el potencial de evolución que puede tener el objetivo planteado con el paso del tiempo, entre otros factores-; sería conveniente una evaluación de impacto que dé cuenta de las consecuencias que podrían derivarse para el titular a partir de tal forma de tratamiento de tales datos por parte de la entidad, de tal forma y con tales fines; además, importa considerar las expectativas razonables del interesado, las deberán concordar con la naturaleza de la relación y/o servicio prestado y, además, se debe tener en consideración el carácter de los datos y los posibles efectos de su tratamiento a escala. Un análisis acucioso de todos estos elementos puede perfilar de mejor manera los mecanismos adecuados de tratamiento de esta información, pudiéndose poner énfasis en aspectos como la confidencialidad, las limitaciones a las cesiones, a los usos posteriores, la implementación de diversos métodos de anonimización y de transparencia, la diferenciación de estándares de seguridad según la sensibilidad de los datos, etc.

- **Aseguramiento del derecho a la impugnación del artículo 8 bis:** Este derecho, que ya fue referido a propósito de las garantías de los titulares, será desarrollado en mayor profundidad en el próximo capítulo de este trabajo.

No conforme con todo lo anterior, este proyecto también se encarga de incorporar otros elementos novedosos en relación con los datos personales, a saber:

- La facultad de los herederos para ejercer los derechos del titular en caso de fallecimiento.
- El deber de los responsables del tratamiento de implementar mecanismos tecnológicos que permitan al titular ejercer sus derechos de manera eficaz, ágil y expedita.
- La gratuidad del ejercicio de los derechos de rectificación, cancelación y oposición y, trimestralmente, el de acceso, pudiendo el responsable generar un cobro si el titular lo ejerce más de una vez dentro de un trimestre. En todo caso, será la autoridad de control la encargada de determinar los costos asociados al ejercicio de cada derecho cuya gratuidad no se encuentre garantizada.

Por último, es necesario recalcar que, para efectos del tratamiento masivo de datos personales, nuestro futuro marco normativo no se conformará con que las formas de tratamiento respondan a los fines compatibles de la entidad, sino que exigirá también la concurrencia de una base de licitud para legitimar el tratamiento. Es decir, señala como requisitos copulativos la existencia de una condición habilitante y un uso acorde a los fines propios de la entidad, con lo que se supera el estándar exigido por el propio RGPD para el cual basta o con una condición habilitante o con un tratamiento ajustado a los fines de la persona jurídica.

2.- Regulación Penal del Big Data:

Para abordar el modo en que esta disciplina del derecho se relaciona con el Big Data, lo primero que es necesario señalar es que el Big Data, como tal, no se encuentra regulado por la legislación penal. En lugar de ello, lo que puede llegar a relacionarse con el tema de este trabajo son los denominados "Delitos Informáticos".

Existe una extensa discusión, no agotada del todo, que busca dilucidar la naturaleza de estas figuras debatiendo si pueden constituir una categoría propia de delito o si son simplemente delitos clásicos en

que se utiliza la informática como herramienta. Al respecto, se ha avanzado en el consenso de que, cuando menos, son conductas necesarias de regular individualmente habida cuenta del grado de riesgo y exposición al que nos enfrentamos a diario debido al impacto del internet en el curso de la vida cotidiana.

Con todo, no parece necesaria una respuesta absolutamente tajante a este asunto, puesto que es posible clasificar los delitos que se cometen haciendo uso de tecnologías de la información en dos categorías: Por un lado, aquellos que históricamente han estado tipificados en la legislación penal pero que hoy pueden llevarse a cabo por medio de herramientas tecnológicas, como las calumnias, amenazas, usurpación de identidad y, aunque es más discutible, algunas formas de hurto o robo, y, por otro lado, los tipos delictivos que se han originado gracias al contexto tecnológico, como ocurre con determinadas formas de vulneración de cuentas, claves, espionaje y sabotaje, así como el *phishing* o la clonación de tarjetas (Migliorisi, 2014).

Tal como ocurrió con la ley 19.628 sobre protección de la vida privada, Chile logró contar tempranamente con una ley de delitos informáticos. En 1991, el Diputado José Antonio Viera-Gallo presentó una moción legislativa a la Cámara de Diputados, dando cuenta de cómo, ya entonces, el "vertiginoso desarrollo de las tecnologías de la información" habían hecho de esta "uno de los más preciados recursos". En la misiva el parlamentario señalaba que "la creciente importancia que ha adquirido la informática ha hecho patente la vulnerabilidad de las sociedades y de las organizaciones que las utilizan", agregando que el proyecto tenía por finalidad "proteger este nuevo bien jurídico que ha surgido con el uso de las modernas tecnologías computacionales: la calidad, pureza e idoneidad de la información en cuanto tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan" (Viera-Gallo, 1991).

Más que calificar al parlamentario como un visionario, la revisión de las palabras que pronunció en aquella época parece dar cuenta, sobre todo, del nivel de retraso con que carga el debate de la regulación informática en la actualidad, ya que, si bien en el año 1993 esta iniciativa logró materializarse en la ley 19.223 sobre delitos informáticos, tras su aprobación cayó prácticamente en el olvido, tal como ocurrió con la ley 19.628 de 1999.

La modesta ley 19.223 cuenta hasta el día de hoy con sólo 4 artículos, cada uno de los cuales tipifica un delito informático que la doctrina ha agrupado en dos grupos: Los delitos de espionaje (artículo 2 y 4) y los delitos de sabotaje (artículos 1 y 3).

Los delitos de espionaje son:

> Artículo 2°: El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.

> Artículo 4°: El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.

Aunque, ciertamente, ambos tipos penales pueden concurrir conjuntamente y tienen un parecido que fácilmente podría prestarlos a confusión, sus elementos difieren como se ve a continuación:

	Ánimo	**Conducta ilícita**	**Objeto**	**Agravante**
Art. 2°	Apoderarse, usar o conocer indebidamente	Interceptar, interferir, acceder	Información contenida en un sistema de tratamiento.	-
Art. 4°	Maliciosamente	Revelar, difundir	Datos contenidos en un sistema de información	Cuando el autor es el responsable del sistema de información

Así, en el caso del artículo 2° el autor busca conocer o apoderarse de los datos para sí; en cambio, en el artículo 4° lo que se condena es la acción de difundirlos para que otros los conozcan, lo cual no requiere indefectiblemente de una interceptación, pudiendo tratarse, por ejemplo, de un funcionario que por el desempeño de su cargo tiene acceso a determinadas bases de datos cuyo contenido debe mantener en reserva.

Además, el artículo 2° tiene la particularidad de disponer una pena incluso para algunas situaciones en las que el autor pudiera no haber logrado obtener la información perseguida. Bien podría ocurrir que el actor interceptara un sistema informático con la intención de apoderarse indebidamente de ciertos datos, pero que, una vez dentro, no lograra hallarlos, por ejemplo, producto de que el sistema hubiese

sido formateado el día anterior. Lo relevante, entonces, no es la obtención de los datos, sino el ánimo y la interceptación del sistema, lo que supone la extraña situación de poderse aplicar una misma pena a aquel que logra su cometido y a aquel que ve frustrado su intento.

Lo que comparten estas figuras corresponde a la dificultad probatoria del ánimo con que se llevan a cabo, ya que en el caso del artículo 2° se debe probar que aquel que interceptó un sistema informático lo hizo con el ánimo de apoderarse de su información, mientras que en el caso del artículo 4° no basta con la mera difusión de los datos, sino que, además, esta debe hacerse en forma dolosa.

Por otro lado, los delitos de sabotaje son:

> Artículo 1°: El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.
>
> Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

> Artículo 3°: El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.

A simple vista, estas figuras parecen más sencillas de distinguir que los delitos de espionaje, toda vez que resulta evidente que el artículo 1° busca proteger la infraestructura, tanto material como lógica, que contiene los datos; mientras que el artículo 3° resguarda la indemnidad de la información contenida en estos soportes. Sin embargo, producto de su redacción, es posible pensar que se pueden superponer ambos tipos penales en aquellos casos en que, producto de una acción maliciosa, se dañan tanto los datos como su soporte, lo que dificulta significativamente la determinación de cuál es el que corresponde aplicar a un caso concreto.

La decisión puede facilitarse si se tiene en cuenta que la agravante del artículo 1° tiene como presupuesto que se hayan dañado los soportes de la información, siendo aplicable sólo cuando, a consecuencia de ello, se genera un menoscabo en los datos del sistema. En contraste, la hipótesis del artículo 3° se sitúa en el evento de que únicamente se produzca un daño en la información.

	Ánimo	**Conducta ilícita**	**Objeto**	**Agravante**
Art. 1°	Maliciosamente	Destruir, inutilizar, impedir, obstaculizar o modificar el funcionamiento.	Sistema de tratamiento de información, sus partes o componentes.	Afectación de los datos contenidos como consecuencia de la conducta anterior.
Art. 3°	Maliciosamente	Alterar, dañar, destruir.	Datos contenidos en un sistema de información.	-

Con todo, caben críticas a la redacción de nuestras figuras de sabotaje. Sobre el artículo 1° se dan principalmente por la aparente confusión que existe sobre el bien jurídico protegido. Si bien es cierto que los delitos informáticos se caracterizan por ser pluriofensivos, afectando aspectos como la privacidad, el patrimonio, la honra, la indemnidad sexual de un menor, entre tantos otros, la redacción del artículo 1° resulta problemática al poner como objeto principal de su protección el soporte que contiene los datos, toda vez que la conducta típica que lleva a tal resultado, es subsumible en el tipo de daños del artículo 484 y siguientes del Código Penal, lo que, en principio, volvería innecesaria la tipificación concreta de esta forma de sabotaje.

Asimismo, resulta criticable la laxitud con que se define el objeto dañado, ya que una interpretación amplia podría llegar a considerar como delito informático la destrucción de un teclado o incluso la del cursor con que se introducen los comandos para el tratamiento de los datos, lo cual constituye un completo absurdo al no existir alteración o manipulación indebida de la información.

En cuanto al artículo 3°, si bien constituye un delito propiamente informático en toda su extensión, ha sido criticado por el excesivo alcance de las conductas que describe y, especialmente, por no graduar la pena en relación con el tipo de tratamiento y la entidad de la información perturbada. De manera que se equipara la alteración de un dato corriente, como podrían ser los relativos a preferencias culinarias, con la destrucción de la base de datos que contiene las fichas sociales de las que depende la entrega de beneficios de una municipalidad. El problema con el sabotaje del artículo 3° es que no logra discernir los niveles de gravedad que importan las diversas formas en que pueden llegar a alterarse distintos tipos de datos.

A pesar de sus falencias, la ley 19.223 es importante para evaluar la regulación penal de algunos usos del Big Data, ya que describe aquellos casos en que el tratamiento de la información se lleva a cabo de manera perniciosa y, por supuesto, ocurre lo propio cuando dichas formas de tratamiento se efectúan en forma masiva.

Así, una operación de *hacking* como la ocurrida en Baltimore durante 2019 permite apreciar los efectos de estas conductas cuando recaen en grandes volúmenes de información crítica para el funcionamiento de, en este caso, una unidad organizacional de un Estado. En relación con el artículo 1°, se inutilizaron maliciosamente numerosos sistemas de tratamiento de información; respecto del artículo 3°, la amenaza consistía en la destrucción de la información si no se pagaba el rescate, que finalmente no fue pagado, por lo que se puede asumir la pérdida de todos los datos secuestrados. En cuanto a los delitos de espionaje, resulta más difícil de aseverar, dado que no conocemos a ciencia cierta si se dio algún tipo de uso a la información a la que lograron acceder; no sabemos si la leyeron, la procesaron, la vendieron o distribuyeron de alguna otra manera, de modo que, por lo pronto, sólo resulta presumible la concurrencia de estas figuras. Esto pone en evidencia lo sensibles que resultan estas conductas para el normal desenvolvimiento de la vida en línea. Cuando este tipo de delitos se efectúan en contra de sistemas críticos de información, es posible llegar a alterar por completo el funcionamiento de un país. Por otro lado, cuando en un nivel más reducido, se cometen en contra de una persona determinada, pueden llegar a tener consecuencias catastróficas para la vida de dicha persona, como ocurre con la "porno venganza" en que se difunden imágenes íntimas de una expareja para perjudicarla (espionaje del artículo 4°).

Como se mencionó anteriormente, el desarrollo jurisprudencial de estos delitos ha sido escaso y bastante errático, aunque vale la pena mencionar que la persecución de estos tipos ha aumentado paulatinamente, sobre todo durante la última década.

De acuerdo con una investigación realizada el año 2014 por la ONG Derechos Digitales, la labor investigativa de los delitos informáticos excede por mucho el ámbito de protección de la ley 19.223, siendo los oficios más abundantes en la BICRIM[4] los relativos a estafas y defraudaciones. Junto con ello, existe gran cantidad de oficios sobre usurpación de nombre, hurto, amenazas, adquisición o almacenamiento de material pornográfico infantil, producción del mismo e, incluso, sobre robos en lugar habitado o por sorpresa, junto con muchos otros, lo que, a todas luces, da cuenta de que el rol de esta unidad especializada ha debido trascender el ámbito de investigación propio de la ley que le da su nombre, abordando por igual conductas que, pese a no constituir la realización de delitos propiamente

[4] Brigada Investigadora del Cibercrimen de la Policía de Investigaciones de Chile (PDI).

informáticos, se valen de estos medios para planificar o llevar a cabo el hecho punible (Lara, Martínez, & Viollier, 2014).

Esta investigación concluye que, si bien, los delitos de la ley 19.223 son escasamente investigados, su imputación ha ido en aumento, pasando de 6 casos formalizados en 2007 a 35 formalizaciones en 2012. No obstante, y a pesar de tratarse de tan pocos casos, los autores llaman la atención acerca de la curiosa circunstancia de que "en los casos en que es usada la Ley de Delitos Informáticos existe una probabilidad mucho mayor de sentencia condenatoria", siendo su porcentaje de condena el de un 92,6% en los casos de espionaje informático y de un 77% para el sabotaje informático en el período de 2006 a 2012, contra el modesto 40,3% de condenas registradas durante el mismo período para la totalidad de delitos judicializados por el Ministerio Público.

Ahora, si analizamos jurisprudencia sobre esta materia, sobre todo de los años en que recién comenzaba a aplicarse esta ley, podemos encontrar diversos errores en que incurrieron los jueces que debieron enfrentar las dificultades de imputar delitos de escasa judicialización respecto de los que no tenían mayor capacitación y que, además, se encontraban contemplados en una ley poco precisa y desactualizada. Todo esto los llevó a confundir los tipos penales aplicables a las conductas que intentaban condenar o a forzar la interpretación de dichas conductas para subsumirlas en una figura que no les correspondía. Algunos ejemplos son:

El 26 de junio de 2009, en causa Rol N°17113(2)-2008, el 7° Juzgado de Garantía de Santiago pronunció una sentencia condenatoria en contra de los miembros de una agrupación criminal por haberse asociado para monitorear las investigaciones desarrolladas por la PDI y generar contra órdenes de detención y arresto, así como para eliminar las órdenes de arraigo y tergiversar otros datos de los sistemas informáticos de la Policía de Investigaciones (PDI) en favor de quien pagará determinadas sumas por ello. Para llevar a cabo estas gestiones, la asociación contaba con funcionarios de la propia institución que se valían de sus claves y las de funcionarios jubilados para consultar, modificar, cancelar e ingresar encargos.

No conforme con ello, esta organización también se encargaba de falsificar sentencias judiciales y resoluciones reconociendo abonos de tiempo en prisión preventiva por causas criminales inexistentes; cambiaban las muestras de sangre en exámenes de alcoholemia y sustraían expedientes para beneficiar a imputados con participación delictiva.

Frente a todos estos hechos, el tribunal condenó a los involucrados por asociación ilícita del artículo 292 del Código Penal, por la interceptación del artículo 2° de la ley 19.223 al estimar que existió acceso a un sistema de información con el fin de conocer y usar indebidamente los datos contenidos en

este y también por la difusión maliciosa del artículo 4° de la ley 19.223 en vista de la información contenida en los sistemas que fue dada a conocer de manera indebida.

Ciertamente es correcta la condena por el espionaje del artículo 2° en tanto se accedió a un sistema de información para conocer y hacer un uso indebido de sus datos. Por supuesto, se podría distinguir entre los casos en que se ingresó con las claves propias de los funcionarios activos de aquellos en que ingresaban con las claves de funcionarios ya jubilados, configurándose accesos ilegítimos sólo en el segundo escenario. Sin embargo, y como veíamos al revisar estos tipos penales, el aspecto que determina la punibilidad de la conducta descrita en el artículo 2° de la ley 19.223 es que el acceso, independiente de cómo ocurra, tenga por objeto hacer un uso indebido de los datos. Es por ello que, para efectos de esta condena, no resulta significativo distinguir cuándo se entraba con las claves propias y cuándo con las ajenas, puesto que en ambos casos se hacía para utilizar los datos del sistema en favor de quienes eran investigados por este cuerpo policial. Asimismo, es efectiva la concurrencia de la difusión maliciosa de información del artículo 4° al dar a conocer a los imputados datos cuya reserva tiene por finalidad lograr una mayor calidad y éxito en las investigaciones.

Lo que llama la atención de este fallo, es la completa omisión de la figura de sabotaje del artículo 3° de esta ley, pues resulta evidente que, en forma maliciosa, se alteraron y dañaron significativamente numerosos datos del sistema de información de la PDI al emitir contra órdenes de arraigo o arresto, al generar abonos de prisión inexistentes para rebajar los cumplimientos efectivos de otras condenas, entre otros, para que la policía no contara con la información necesaria para seguir adelante con las investigaciones respectivas.

De manera que el tribunal sólo logró elucidar la concurrencia de los delitos de espionaje sin percatarse siquiera de los actos de sabotaje configurados y verificados en el caso.

Por otro lado, el fallo pronunciado por el 8° Juzgado de Garantía de Santiago el 11 de marzo de 2008 en causa Rol N°3665-2007, condenó al imputado extendiendo la aplicación del artículo 2° de la ley 19.223 a conductas que no eran subsumibles al tipo penal. En este caso, el imputado obtuvo la clave de acceso a la cuenta bancaria de un tercero y efectuó una transferencia de dinero a una tienda de artículos tecnológicos para comprar determinados productos. A continuación, se comunicó con la empresa y confirmó haber realizado la transferencia, dio un nombre falso y retiró los productos en el local. No obstante, fue detenido por personal de la PDI cuando salía con las compras, puesto que ya se había efectuado la denuncia.

El autor fue condenado por los delitos de estafa de los artículos 468 y 467 n°2 del Código Penal, usurpación de nombre del artículo 214 del mismo cuerpo legal y *"fraude informático"* del artículo 2° de la ley 19.223. En la acusación, el fiscal señaló que el engaño utilizado para obtener los productos

configuraría la estafa calificada de los artículos 468 y 467 n°2 del Código Penal, pero no se encuentra ninguna explicación de cómo los hechos habrían configurado una defraudación informática ni sobre cómo podría imputarse un fraude informático por medio del artículo 2° de la ley 19.223. Al tratarse de un juicio abreviado, en que existió una aceptación de los hechos por parte del imputado, no se presentó mayor debate jurídico en relación con estas calificaciones. Así, el juez no hizo más que referir dichas calificaciones en la sentencia sin ahondar en el por qué de sus conclusiones.

Con todo, la sentencia resulta interesante porque, sin pretenderlo, llama la atención acerca de las falencias de la norma. Es decir, en circunstancias en que el delito "informático" que más se investiga por nuestras policías es el de fraude, resulta problemático que no exista una figura penal que lo tipifique.

Estas formas de defraudación, en la mayor parte de los casos, no pueden subsumirse siquiera en la figura de estafa residual del artículo 473 del Código Penal, toda vez que, al tratarse de un delito que la doctrina ha entendido como de autolesión, los presupuestos mínimos para que esta opere son el engaño por parte del autor, el error consecuente en la víctima, la disposición patrimonial por parte de la víctima y, junto con ella, el perjuicio autoinfligido. Así, en la medida que no sea la propia víctima la que se figura una falsa representación de la realidad y, producto de ella, realiza la disposición patrimonial que la perjudica, no es posible hablar en forma estricta de ninguna de las figuras de estafa contempladas en el derecho positivo chileno, de modo que denominar estafa o defraudación a la vulneración o aprovechamiento de algún sistema informático para realizar, de propia mano, una transferencia en perjuicio de otro, constituye una imprecisión jurídica que, no obstante, se ha empleado malamente en un intento de subsanar las deficiencias de nuestra legislación.

Aunque no se especifica de qué manera el autor obtuvo la clave de la cuenta bancaria de la víctima, se puede afirmar que la figura penal aplicable es una que todavía tiene un carácter meramente doctrinario en nuestro país, a saber, el *phishing*, que consiste básicamente en el robo de datos personales, o bien, en la obtención fraudulenta de datos, claves de cuentas bancarias, números de tarjeta de crédito, y demás antecedentes, con el objeto de ser posteriormente utilizados en lugar de su titular, ya sea en perjuicio del mismo o de un tercero (Rosenblut, 2008).

En definitiva, no existe tipificación penal adecuada en la legislación chilena para delitos como la estafa o defraudación informática, el *phishing* y el *pharming*[5], que corresponden a algunas de las figuras más habituales de vulneración de sistemas informáticos. Estas conductas, sin embargo, son investigadas y perseguidas penalmente por el Ministerio Público, pero para ser imputadas, se tratan de amoldar a otros

[5] Ciberataque que consiste en el redireccionamiento de una página web a otra falsa, generalmente con la finalidad de obtener los datos que normalmente depositaría el usuario en la página web original, como datos personales, claves u otros.

tipos penales contemplados por el ordenamiento, como son las estafas residuales, el hurto o imprecisiones como el *"fraude informático"* que se logra forzando el artículo 2° de la ley 19.223.

Es claro que, individualmente considerados, ninguno de estos delitos da cuenta de una forma de tratamiento masivo de datos. Sin embargo, la programación de algoritmos dirigidos en forma intensiva a un extenso listado de direcciones para recabar datos de utilidad para futuras defraudaciones, para inhabilitar sistemas informáticos, para solicitar rescates a cambio de no divulgar la información obtenida o devolver el acceso a sus respectivas bases de datos son hipótesis que, a nivel macro, sí revisten importancia y peligrosidad a la hora de pensar una adecuada regulación del Big Data. Lo propio ocurre cuando las bases de datos que son atacadas contienen importantes volúmenes de información capaz de afectar a grandes números de personas o servicios de utilidad para la población.

Sirve a estos efectos destacar el aumento de ataques informáticos que se han evidenciado en el marco de la pandemia que aqueja al mundo en estos momentos. La necesidad de imponer cuarentenas como medida de protección frente a la enfermedad, ha llevado a un incremento en las conexiones privadas a la web. El teletrabajo, ha supuesto que millones de personas deban desempeñar desde sus hogares las funciones que normalmente llevaban a cabo en dependencias de sus respectivas oficinas y con sistemas de protección más sofisticados que aquellos a los que puede acceder cada empleado para protegerse de los ciber ataques desde su casa. Así, se acrecientan las brechas de seguridad y los puntos de vulnerabilidad explotables para acceder a los datos que busca proteger una empresa u organismo público. Junto con ello, la falta de actividades que deriva en un mayor tiempo frente a las pantallas parece facilitar el que las personas caigan en distintos tipos de engaños destinados a obtener datos, claves o disposiciones patrimoniales lesivas a través de internet.

Durante el primer semestre de 2020 fuimos testigos del ataque a las bases de datos de la aerolínea EasyJet, de donde se sustrajeron los correos electrónicos de alrededor de 9 millones de clientes junto la información relativa a sus viajes y los datos de 2.208 de sus tarjetas de crédito (Gold, 2020); más grave aún, la compañía británica de *software* SOPHOS, realizó un estudio independiente en el que encuestó a 5.000 empresas de tecnología pertenecientes a un total de 26 países, de las cuales el 51% declaró haber sido víctima de un ataque vía *ramsomware* sólo durante 2020 (SOPHOS, 2020).

Por otro lado, en Chile, la Brigada del Cibercrimen de la PDI sostuvo haber recibido alrededor de 500 denuncias al día. El subprefecto Luis Orellana, jefe de la Brigada, señaló en mayo de 2019 que los delitos de *phishing*, las falsas ofertas y las solicitudes de información han aumentado, agregando que "Los ciberdelincuentes envían estafas hasta que alguien caiga". De acuerdo con la institución, se trataría de delitos que se van adaptando a las circunstancias de la contingencia (Cerna, 2020).

Este incremento fue tan evidente durante la pandemia que, advirtiendo los riesgos que se podían derivar de este aumento en los casos y su sofisticación, el Servicio Nacional del Consumidor (SERNAC) se vio en la necesidad de elaborar decálogos y distintos mecanismos para advertir a la ciudadanía de la diversificación de estos métodos, sus ámbitos de mayor ocurrencia, cómo prevenirlos y cómo denunciar (SERNAC, 2020).

Sin lugar a dudas, este sensible aumento en la cibercriminalidad enciende alarmas en un momento en que las sociedades han debido volcarse de manera abrupta hacia las tecnologías de la información, volviéndose más dependientes de ellas que nunca antes en la historia. Este escenario de híper conectividad convierte en un imperativo la inmediata necesidad de avanzar tanto en la regulación como en las medidas y herramientas efectivas de protección para el tráfico de información en la web, por lo que, no cabe duda, este será uno de los grandes debates de los próximos años.

Sin perjuicio de lo anterior, y previo a la pandemia, ya existían avances significativos en la regulación de esta materia. Avances que, tal como en el caso de la protección de los datos personales, tuvieron su origen en la Unión Europea y se materializaron el año 2001 en el Convenio de Budapest.

El Convenio de Budapest surge como respuesta a la necesidad palpable de generar mecanismos de cooperación internacional para luchar contra el cibercrimen y para definir con mayor precisión las actividades que constituyen una amenaza en la red. Junto con ello, supone un salto cualitativo en el proceso de unificación legislativa de los países signatarios, factor de suma relevancia a la hora de enfrentar el cibercrimen.

Este esquema de colaboración entiende que un ciberdelincuente puede enviar un ataque desde el país A para capturar datos pertenecientes a una persona que reside en el país B, pero que, no obstante, se encuentran almacenados en un servidor ubicado en el país C que presta servicios de almacenamiento a la compañía responsable de la información cuyas oficinas se hallan en el país D. Además, el ciberdelincuente podría pedir un rescate a una cuenta o monedero virtual ubicado en el país E para recuperar o no publicar los datos.

Si frente a tal escenario cada país optara por aplicar de manera estricta el principio de territorialidad, sería imposible perseguir este tipo de ataques en todas sus dimensiones. Podría haber 5 cuerpos policiales realizando las mismas labores investigativas y se generarían choques de jurisdicción y problemas de extradición a la hora de determinar dónde debiera seguirse el juicio contra los autores. No conforme con ello, el embrollo de intentar armonizar 5 legislaciones diversas sobre la materia llevaría a cada Estado a sostener una versión diversa sobre los mismos hechos y, finalmente, sería sumamente complejo llegar a un acuerdo sobre qué, cómo y dónde imputar, por lo que, seguramente, cada Estado

sancionaría el pedacito que aconteció en su territorio o, derechamente, sobreseerían algunas de las conductas por no constituir delito, como podría ocurrir con una mera transferencia electrónica.

En sus 4 capítulos, el Convenio de Budapest establece una terminología común; genera un catálogo de medidas a seguir para los países signatarios, entre las que se incluye la tipificación de las conductas sancionadas por el Tratado, distinguiendo entre delitos contra la confidencialidad, delitos informáticos, delitos relacionados con el contenido, delitos contra la propiedad intelectual y otras formas de responsabilidad, junto con la especificación de los aspectos procesales a implementar para lograr la aplicación de la norma dentro de un territorio nacional; dispone los mecanismos de cooperación internacional y asistencia mutua mediante los cuales una institución designada por cada país podrá solicitar a su homóloga en el extranjero que se adopten distintas medidas precautorias respecto de ciertos datos, evitando que las bases de datos sean eliminadas mientras se consiguen los permisos para acceder a tal información, entre otras medidas.

Aunque no es el objetivo de este trabajo analizar el Convenio de Budapest en forma pormenorizada, sí parece necesario abordar brevemente sus aportes más destacables:

a) Genera una homologación terminológica sobre conceptos mínimos, a saber, "sistema informático", "datos informáticos", "proveedor de servicios" y "datos sobre el tráfico".
b) Establece una categorización de los distintos tipos de delitos que pueden cometerse en o a través de sistemas informáticos. Estos son: Delitos contra la confidencialidad, Delitos informáticos, Delitos relacionados con el contenido y Delitos relacionados con infracciones a la propiedad intelectual.
c) Introduce formalmente los delitos de falsificación informática y de estafa informática dentro de la categoría de los delitos informáticos propiamente tal.
d) Introduce delitos cuya gravedad está puesta en su contenido. Esto refiere específicamente a los delitos relativos a la pornografía infantil que se cometen haciendo uso de sistemas informáticos o con el objetivo de poner dicho material a disposición, tanto propia como de otros, por medio de sistemas informáticos.

   La incorporación de este tipo de delitos es sumamente relevante, ya que, si bien todas las legislaciones contienen tipos penales que castigan la creación y difusión de pornografía infantil, no se había abordado de manera adecuada la estrecha relación de esta clase de delitos con las tecnologías que, finalmente, son los motores que facilitan y promueven este material a través de la web, donde suelen generarse grandes organizaciones dedicadas a la explotación sexual infantil que, en la actualidad, deben ser perseguidas mucho más por medios informáticos que a través del mundo analógico.

e) Establece otros regímenes de responsabilidad. Esto aborda dos aspectos: Por un lado, establece responsabilidad para quienes participen de varios de los delitos detallados en el Convenio, ya sea en calidad de cómplice o en grado de tentativa y; por otro lado, establece responsabilidad para las personas jurídicas cuando una persona física con poder de representación, toma de decisiones o actuación cometa alguno de los delitos descritos en el Convenio a nombre de la persona jurídica o permita su comisión por falta de la debida vigilancia. Con todo, queda al arbitrio de los países firmantes determinar si la responsabilidad atribuida a las personas jurídicas ha de ser de carácter civil, penal o administrativa.

f) La adopción de un sistema de conservación rápida de datos almacenados que consiste en dotar a un determinado organismo con la autoridad para imponer a los proveedores de servicios informáticos la conservación inmediata de determinados datos, debiendo mantener secreto de este procedimiento, cuando existan razones para creer que estos son especialmente susceptibles de pérdida o deterioro. El Convenio dispone que esta conservación debe poder dictarse al menos por 90 días, de modo que la autoridad competente tenga la posibilidad de obtener las autorizaciones necesarias para poder acceder a la información. Asimismo, se instaura un sistema de conservación y revelación rápida de datos de tráfico que permiten identificar las características que rodean la información principal y su respectivo proveedor.

   Junto con ello, se dictan criterios y determinadas hipótesis bajo los cuales la autoridad competente estará facultada para interceptar comunicaciones y grabarlas en tiempo real con la colaboración de los proveedores de servicios.

g) Se establecen algunos criterios de jurisdicción y extradición para determinar cuándo un Estado tiene prioridad para perseguir un delito informático que le haya afectado, promoviendo el máximo de cooperación internacional al efecto.

h) Teniendo en cuenta las dificultades para conseguir la realización de diligencias investigativas en el extranjero y la velocidad con que puede desaparecer la información relativa a los delitos informáticos, el Convenio flexibiliza los requisitos necesarios para otorgar validez a una solicitud de información o de determinados procedimientos requerida por la autoridad competente de otro de los países signatarios, validando "medios rápidos de comunicación", como el teléfono, correo electrónico, fax u otros, para pedir determinadas gestiones siempre que cuenten con sistemas de seguridad y autenticación adecuados.

   Una vez recibidas estas formas de comunicación, el país requerido ha de proceder a la realización del trámite en conformidad con su derecho interno.

   Entre las gestiones posibles de solicitar se encuentran la retención o conservación de determinados datos que puedan llegar a ser confiscados cuando el requirente cuente con todos

los permisos correspondientes para acceder a ellos, la entrega de los datos de tráfico referidos a una comunicación específica y la interceptación en tiempo real tanto de datos de tráfico como de contenido.

i) La creación de una Red 24/7 que permita la comunicación y coordinación de las autoridades de control las 24 horas del día los 7 días de la semana con el objeto de garantizar la prestación de ayuda inmediata para los fines de investigaciones o procedimientos **relacionados con delitos vinculados a sistemas informáticos, o para la obtención de pruebas electrónicas de un delito**. De modo que el rol de la Red 24/7 trasciende a los delitos establecidos en el catálogo del Convenio de Budapest y permite la asistencia técnica, la realización de diligencias de conservación de datos y la obtención de pruebas en el marco de, básicamente, cualquier investigación penal que involucre la utilización de sistemas informáticos, como podría ocurrir, por ejemplo, con un secuestro en que el secuestrador pida un rescate por medio de un servicio de mensajería móvil como WhatsApp.

Mucho tiempo después del nacimiento de este Convenio, Chile advirtió el profundo déficit normativo y de implementación que padecía el país en materia de ciberseguridad. El tema comenzó a desarrollarse primero como materia de investigación académica en reducidos nichos, pero con el pasar del tiempo se hizo evidente la necesidad de llenar estos vacíos y generar tanto una legislación como un sistema de ciberseguridad adecuados para enfrentar los riesgos de la era de las comunicaciones.

Uno de los grandes hitos en este sentido ocurrió el 16 de noviembre de 2016, cuando el Congreso Nacional aprobó el Convenio de Budapest que fue promulgado posteriormente, el 27 de abril de 2017.

El mismo 27 de abril de 2017, la Presidenta de la República Dra. Michelle Bachelet dio a conocer una Política Nacional de Ciberseguridad sosteniendo que "La discusión sobre ciberseguridad resulta esencial para el desarrollo y el fortalecimiento de los valores de la democracia, el respeto al derecho internacional y la protección de los derechos fundamentales de las personas" (Silva, 2017). Entre los objetivos de este proyecto estaban la implementación de una infraestructura de la información resiliente, capaz de resistir y responder en caso de ataques informáticos, siendo necesario establecer para ello un marco normativo y de obligaciones respecto de la infraestructura crítica del país, tecnificándose los protocolos y ámbitos de gestión de riesgos. Otro de los pilares de este proyecto era el de velar por el cuidado de los derechos de las personas en el ciberespacio, entendiendo su relevancia no sólo a nivel institucional, sino también en tanto ciudadanos, para lo que se volvía indispensable promover una industria de la ciberseguridad y el desarrollo de capital humano avanzado en esta materia. Además, se apuntaba a la educación y capacitación de la población respecto de las buenas prácticas en materia digital,

poniendo énfasis en la población vulnerable, a saber, niños, niñas y personas mayores, con miras a crear una cultura de la ciberseguridad (Gobierno de Chile, 2017).

Este proyecto, que se fijaba metas a mediano y largo plazo, tenía el objetivo de que para el año 2022 Chile tuviera operativa su primera estrategia de ciberseguridad.

Concluido el período presidencial de Michelle Bachelet, el gobierno de Sebastián Piñera decidió dar continuidad a esta iniciativa mediante a denominada "Estrategia Nacional de Ciberseguridad", que tuvo uno de sus hitos más relevantes el día 25 de octubre de 2018, fecha en que se presentó el proyecto de ley de delitos informáticos que busca derogar la ley 19.223.

Este proyecto busca modernizar los parámetros de persecución de los delitos informáticos adaptándolos a los estándares establecidos en el Convenio de Budapest.

Con fecha 21 de marzo de 2022, y tras largas discusiones, se aprobó el último informe de la Comisión Mixta que tenía por objecto resolver las diferencias que se habían generado entre el Senado y la Cámara de Diputados durante la tramitación de este proyecto, por lo que el 22 de marzo de 2022 se ofició al Ejecutivo a fin de saber si el Presidente de la República ejercerá su derecho a veto. A la fecha en que se escriben estas líneas, esta misiva sigue pendiente de contestación, por lo que entendemos que el proyecto de ley aprobado debiera ser publicado y ser ley, por lo que, a continuación nos referiremos a sus normas en lo que es pertinente a nuestra investigación:

a) Título I: De los Delitos Informáticos y sus Sanciones:

Se extiende la tipificación penal de 4 a 8 figuras de delitos informáticos y se establecen las circunstancias atenuantes y agravantes de responsabilidad. Así, se prevén los siguientes delitos informáticos:

i. Ataque a la Integridad de un Sistema Informático: Sanciona a quien obstaculice o impida total o parcialmente el normal funcionamiento de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos.

ii. Acceso Ilícito: Sanciona a aquel que, sin autorización, o excediendo la autorización que posee, y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático.

> Además, agrava la pena cuando el ilícito se comete con el ánimo de apoderarse o usar la información contenida y se penaliza de igual modo al tercero que divulgue la información a la que se accedió de manera ilícita aun cuando no fuera obtenida por este.
>
> Por último, se penaliza con uno a dos grados adicionales a quien obtenga y divulgue la información de manera ilícita.

Sin lugar a duda, esta norma suscitó el mayor debate entre congresistas y expertos. Tras la presentación de diversas formulaciones para el ilícito, se debió reflexionar acerca de sus alcances. En este sentido, se cuestionó a partir de cuándo se puede considerar ilícito el acceso, es decir, desde el mero acceso, cuando la intencionalidad es lesiva o en todos los casos en que no exista una eximente de responsabilidad.

Ante esta discusión, se planteó explicitar una eximente de responsabilidad penal para los investigadores informáticos que, en virtud de su trabajo o de la enseñanza y aprendizaje de este campo, accedan sin autorización a sistemas informáticos sin causar daño ni aprovecharse de la información contenida en ellos. Con esto, sostenían, se podría evitar el desincentivo para el desarrollo y capacitación de esta disciplina que fácilmente podría comenzar a ser perseguida, pese a su necesidad, por convertir la actividad en un delito sin distinguir quién la realiza, cómo ni para qué.

No obstante, se opusieron a la incorporación de esta eximente el Ministerio del Interior y el Ministerio Público, señalando este último que su creación daría pie a su utilización masiva por parte de los abogados defensores que, cuando menos, tratarían de construir la eximente incompleta para lograr una atenuante que disminuyera la pena en un grado, haciéndola pasar de una multa a la completa impunidad. Una situación como esta, sostuvieron, convertiría en letra muerta la tipificación del acceso ilícito, por lo que propusieron que tal eximente fuera regulada en una ley administrativa posterior y no en el proyecto de ley en discusión, lo que conlleva desentenderse del problema en lo inmediato y convertir en delito los accesos no autorizados que los investigadores informáticos necesitan realizar para la enseñanza y ejercicio de su profesión.

Aunque hubo quienes trataron de salvar la eximente proponiendo alternativas como un registro de investigadores informáticos, la condición de no causar daño, la obligación de informar de inmediato acerca de las vulnerabilidades detectadas y la prohibición de aplicar la eximente incompleta, finalmente se optó por no incorporarla a esta norma, renunciando con ello a convertir a Chile en el país pionero en regular este asunto de manera explícita, ya que, siguiendo los parámetros del Convenio de Budapest, los países que cuentan con legislación relativa a los delitos informáticos no han incorporado una eximente de estas características.

Sin perjuicio de lo anterior, desde la óptica procesal, atendido que la norma no es una prohibición sino que impone un requisito, los investigadores deberán, previo a sus actividades, celebrar acuerdos y

atenerse a los términos que se establezcan en dichos instrumentos. Dado el tenor de la norma, según el cual la hipótesis señala el que "sin autorización, o excediendo la autorización que posee, y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático", entendemos que la carga de la prueba de probar que cuenta con la autorización y los términos de la misma, mientras que al ofendido le corresponderá acreditar que se superaron las barreras técnicas o medidas tecnológicas de seguridad.

i. Interceptación Ilícita: Sanciona al que indebidamente intercepte, interrumpa o interfiera, por medios técnicos, la transmisión no pública de información en un sistema informático o entre dos o más de ellos; también penaliza a aquel que, sin la debida autorización, capte por medios técnicos los datos contenidos en sistemas informáticos a través de sus emisiones electromagnéticas.

En este caso, también se incluyen condiciones para que la interceptación sea ilícita, la primera es que "indebidamente" comenta las conductas de intercepción, interrupción o interferencia; en segundo lugar, "sin la debida autorización", respecto de las conductas de captar por medios técnicos los datos contenidos en sistemas informáticos.

ii. Ataque a la Integridad de los Datos Informáticos: Sanciona al que indebidamente altere, dañe o suprima datos informáticos.

iii. Falsificación Informática: Sanciona al que indebidamente introduzca, altere, dañe o suprima datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar datos auténticos. La pena asociada a esta conducta se agrava en el caso de los funcionarios públicos que abusan de su oficio para llevar a cabo esta alteración de los datos.

iv. Receptación de Datos Informáticos: Sanciona a quien, conociendo su origen o no pudiendo menos que conocerlo, comercialice, transfiera o almacene, a cualquier título y con cualquier fin, datos informáticos provenientes de un acceso ilícito, una interceptación ilícita o una falsificación informática. En estos casos, se aplicará la pena del delito respectivo rebajada en un grado.

La figura de receptación de datos informáticos no se encontraba originalmente contemplada en este proyecto de ley, sino que fue incorporada durante su tramitación.

Al debatir estos ilícitos, y en particular en la discusión sobre la falsificación informática, el Ministerio Público expuso que "lo usual es que quien falsifica no sea el mismo sujeto que se aprovecha del ilícito", por lo que recomendó establecer una figura de receptación de datos que pueda dar cuenta del uso posterior de los datos obtenidos de una alteración, del acceso indebido, de la falsificación o defraudación de sistemas informáticos. Lo propio se explicó respecto del acceso y la interceptación ilícita, puesto que para estos casos suele identificarse a quien usa y se beneficia de los datos, mas no a quien realizó la actividad ilícita para obtenerlos.

La creación de esta figura de receptación busca combatir el comercio de datos informáticos obtenidos de manera ilícita, al establecer un tipo penal que sanciona a aquellos que se benefician de su obtención y que, hasta ahora, han podido operar sin riesgos, ya que al ser descubiertos no tienen ningún incentivo para colaborar con la investigación puesto que son conscientes de no arriesgar condena alguna.

v. Fraude Informático: Sanciona al que, causando perjuicio a otro y con la finalidad de obtener un beneficio económico para sí o un tercero, manipule un sistema informático mediante la introducción, alteración, daño o supresión de datos o a través de cualquier interferencia en el funcionamiento de un sistema informático.

Para estos casos, el valor de la condena se determinará a partir de la cuantía del perjuicio económico causado, respondiendo a una de las principales críticas a la actual ley de delitos informáticos.

Igualmente, se sanciona como si fuera autor a aquel que, conociendo o no pudiendo menos que conocer la ilicitud de la conducta, facilite los medios para cometer este delito.

Es relevante señalar que gracias a la incorporación de este tipo puede salvarse la persecución penal de las conductas de manipulación de dispositivos informáticos con el objeto de obtener un beneficio económico que en la actualidad malamente se intentan subsumir bajo la figura de estafa. El fraude informático se distingue de la estafa puesto que no existe engaño a una persona, sino manipulación de sistemas informáticos en perjuicio de una persona. Además, la disposición patrimonial lesiva no la realiza la víctima, como ocurre en la estafa producto del engaño, sino que se produce a consecuencia de la alteración o manipulación del sistema informático.

Un aspecto que llama la atención es el inciso tercero de este artículo, en que, a solicitud del Ministerio Público, se determinó elevar al cómplice o receptor a la calidad de autor

del delito de defraudación informática. Para estos efectos se estimó que este partícipe se encuentra dentro del curso causal del delito toda vez que no puede existir una defraudación informática sin una persona que reciba en una cuenta propia el dinero obtenido. Aquel que presta su cuenta para recibir el dinero, pese a ser más fácil de hallar, en la actualidad no es posible de sancionar por la gran dificultad probatoria del concierto previo, de modo que se logra salvar este impase generándole, además, un incentivo para colaborar con la investigación del ilícito principal.

vi. Abuso de Dispositivos: Sanciona al que, para perpetrar los delitos de ataque a la integridad de un sistema informático, acceso ilícito, interceptación ilícita o ataque a la integridad de datos informáticos o que, para cometer los delitos del artículo 7 de la ley 20.009,[6] entregare u obtuviere para su utilización, importare, difundiera o pusiera a disposición de otra forma uno o más dispositivos, programas computacionales, contraseñas, códigos de seguridad o de acceso u otros datos similares, creados o adaptados principalmente para la perpetración de dichos delitos.

Lo que suscitó discusión en relación con este delito fue la amplitud de las conductas típicas, dado que se penaliza la mera tenencia o tráfico de herramientas que sirven para la comisión de los delitos señalados en el párrafo anterior. En este sentido, el Profesor Alejandro Hevia advirtió que la instrucción de profesionales de la ciberseguridad requiere de la utilización dispositivos cuyo objetivo es el *hackeo*, lo que pone en riesgo a estudiantes e investigadores que posean estos elementos, perjudicando su debido entrenamiento y la innovación en esta área del conocimiento.

Sin embargo, el Profesor Daniel Álvarez, el Jefe de Asesores Pablo Celedón y Ministerio Público sostuvieron que este aspecto se encuentra cubierto por la norma en tanto establece una condena sólo para quienes obtengan o distribuyan estos dispositivos para perpetrar los delitos señalados, circunstancia que también debe ser probada.

Lo que se pasa por alto en esta argumentación es que, como vimos, en el tipo de acceso ilícito se optó por eliminar la eximente de responsabilidad para investigadores informáticos, logrando que, básicamente cualquier vulneración no autorizada de sistemas informáticos pase a ser constitutiva de delito, de modo que podría llegar a asumirse en muchas circunstancias que la mera tenencia de este tipo de dispositivos no puede sino estar destinada a la vulneración no autorizada de sistemas informáticos, práctica que pasaría a ser ilegítima para todos los casos con la aprobación de esta ley, criminalizando así

[6] Uso fraudulento de tarjetas de pago y transacciones electrónicas.

aspectos esenciales de la enseñanza y aprendizaje de un importante conjunto de habilidades informáticas que, en definitiva, podría inhibir su actividad.

Además, en este Título se establece la atenuante de colaboración eficaz con la investigación a fin obtener información sobre la persona u organización que orquesta este tipo de ilícitos y no sólo acerca de quienes contribuyen como su último eslabón, pudiendo aplicarse también si dicha colaboración sirve para prevenir o impedir la perpetración o consumación de otros delitos de igual o mayor gravedad contenidos en esta ley.

Por otro lado, se contemplan las agravantes de cometer los ilícitos abusando de una posición de confianza o deber; cuando se cometen abusando de la vulnerabilidad, confianza o desconocimiento de niños, niñas, adolescentes o adultos mayores, y cuando, como resultado de estas conductas, se afecten o interrumpan servicios de utilidad pública o el normal desenvolvimiento de los procesos electorales.

b) Título II: Del Procedimiento:

En este acápite se otorgan mayores facultades investigativas al Ministerio Público, permitiéndole, cuando resulte imprescindible y existan sospechas fundadas contra una persona, solicitar al Juez de Garantía que ordene la realización de las técnicas investigativas previstas en los artículos 222 a 226 del Código Procesal Penal, esto es, la interceptación de comunicaciones telefónicas o de otras formas de telecomunicación, su registro, la fotografía, filmación u otros medios de reproducción de imágenes conducentes al esclarecimiento de los hechos y la grabación de comunicaciones entre personas presentes.

Tales herramientas pueden resultar sumamente útiles para prevenir y lograr el esclarecimiento de este tipo de ilícitos que, a la fecha, no permiten siquiera la interceptación de telecomunicaciones entre dispositivos, sino sólo el acceso a sus contenidos una vez que han sido incautados.

Junto con ello, se faculta al Ministerio Público para que, previa orden del Juez de Garantía, ordene a funcionarios policiales actuar bajo identidad supuesta (de encubierto) en comunicaciones desarrolladas por medio de canales cerrados a fin de esclarecer los hechos constitutivos de estos delitos, la identidad de sus partícipes, la comisión de los delitos, o bien, para impedirlos. Para ello, y siempre que sea necesario para la investigación, el agente podrá incluso intercambiar, enviar o recibir por sí mismo archivos de contenido ilícito, lo que no podrá constituir una circunstancia atenuante para el imputado.

c) Título III: Disposiciones Finales:

En contraste con otras leyes que comienzan con un catálogo de definiciones, este proyecto las incorpora recién en su artículo 15, definiendo datos informáticos, sistemas informáticos y prestaciones de servicios de acuerdo con los lineamientos del Convenio de Budapest.

Mediante un texto carente de propósito, el artículo 16 termina de cerrar las puertas a una eximente de responsabilidad para investigadores informáticos en relación con el delito de acceso ilícito, ya que se establece explícitamente que sólo contará con autorización para acceder a estos sistemas aquel que, en el marco de una investigación de vulnerabilidad o para mejorar la seguridad informática, acceda mediando autorización expresa de su titular. Teniendo en cuenta que el artículo 2 sanciona al que accede a un sistema informático sin autorización, la incorporación de este artículo carece de toda utilidad.

Este título también incorpora otras de las facultades contenidas en el Convenio de Budapest, como la posibilidad de ordenar a los proveedores preservar los datos en forma provisoria a petición del Ministerio Público en el marco de una investigación penal de cualquier índole hasta por 180 días en tanto se autoriza el acceso a los contenidos y obligando a los proveedores a colaborar y mantener esta diligencia en secreto.

La aprobación de esta ley traerá consigo una diversificación de los delitos informáticos que contarán ahora con una descripción detallada y precisa para cada caso y, además, un conjunto de herramientas que no son aplicables hoy y que permitirán investigaciones más efectivas, no sólo para los delitos de carácter informático, sino también para aquellos, de toda índole, en que se ha tratado información relevante en sistemas informáticos.

Complementando lo anterior, en octubre de 2021 el Ministerio de Ciencia, Tecnología, Conocimiento e Innovación lanzó su "Estrategia Nacional de Inteligencia Artificial" que pretende dar un salto en la forma en que funciona el Estado, en su relación con los ciudadanos y, a su vez, en las formas de relación posibles al interior de la misma ciudadanía (Comisión Desafíos del Futuro, Ciencia, Tecnología e Innovación, 2019) (Ministerio de Ciencia, Tecnología, Conocimiento e Innovación, 2022).

Por lo pronto, baste mencionar que este proyecto busca acompañar los avances en materia de modernización del Estado, la aprobación de la nueva ley de protección de datos personales y el observatorio de datos que intenta implementar el Ministerio de Economía para fines científicos y tecnológicos.

Pese al retraso que han sufrido iniciativas en materia tecnológica que gozaban de bastante prioridad hasta hace algunos años, en el curso de esta pandemia, hemos sido testigos de numerosos proyectos que requieren de grandes cantidades de información para generar modelaciones, predicciones, sistemas de trazabilidad de contagios, estimaciones de la capacidad de respuesta de los centros hospitalarios y un largo etcétera, que han puesto en el debate, sobre todo atendiendo a la ineficaz

regulación informática con que Chile enfrenta este escenario, la contingente necesidad de sacrificar la privacidad en pos de obtener una mayor masa de datos que permitan dar respuesta a interrogantes como las señaladas.

3.- Caso de Estonia

Para contrastar el caso chileno y adentrarnos en alternativas para abordar el big data desde una perspectiva procesal de manera más pormenorizada, concluiremos este capítulo refiriendo la regulación estonia, puesto que este país ha dado un salto cualitativo en términos de la aplicación del big data en diversos ámbitos de la administración pública, llegando a ser considerado por la revista Forbes el año 2020 como el país más digitalizado del mundo (Cerdeira, 2020).

En esta avalancha de innovación que caracteriza a este país europeo, y dentro del campo jurídico, Estonia dio una sorpresa al mundo el año 2019 al anunciar la incorporación de jueces robot provistos de sistemas de inteligencia artificial para fallar causas de baja cuantía (hasta 7000€), con el objeto de perfeccionar su razonamiento a fin de poder utilizarlos para solucionar controversias de mayor envergadura el día de mañana. Al menos durante su fase de implementación, los fallos emitidos por este tipo de sistema serán apelables para que resuelva un juez humano (Estonia se prepara para tener "jueces robot" basados en inteligencia artificial, 2019).

Naturalmente, para hacer frente a tamaña adaptación en su sistema judicial, fue fundamental establecer parámetros adecuados de seguridad y cumplimiento que pudieran velar en todo momento por las garantías de las personas durante la tramitación de sus causas. Es por ello que el estudio del caso estonio reviste tal interés en la actualidad.

El Acta de Protección de Datos Personales de Estonia aborda en su cuarto capítulo el tratamiento de datos personales por parte de las autoridades encargadas del cumplimiento normativo para prevenir, detectar y procesar ofensas y para ejecutar sanciones. Con miras a este objetivo, que corresponde al fin específico del tratamiento, este cuerpo normativo establece los siguientes principios:

- Legalidad y justicia en el tratamiento de los datos.
- Finalidad o propósito, vale decir, que el tratamiento de la información debe estar siempre orientado al cumplimiento de un objetivo concreto y determinado.
- Calidad de la información y evitación del uso de datos excesivos.
- Precisión.

- Retención en un formato que permita identificar al titular sólo en la medida necesaria para cumplir el fin del procesamiento de los datos.
- Seguridad de la información.

Como se puede apreciar, estos principios resultan muy afines a los planteados tantos por el RGPD como por el proyecto de ley que se tramita en Chile, pero parecen un tanto más restrictivo para esta función en tanto enfatizan el uso legal, justo y no excesivo de los datos.

En esta línea, los segundos usos de la información que no sean consentidos y que tengan un propósito diverso al de prevenir, detectar y procesar ofensas o ejecutar condenas por parte de las autoridades encargadas del cumplimiento de la ley, se permiten sólo cuando el controlador tenga motivos conformes con la ley o con la legislación de la UE para operarlos con estos nuevos fines o cuando esta normativa lo requiera en la medida que la finalidad perseguida sea proporcional al nuevo uso.

A fin de preservar los derechos de los titulares, las autoridades encargadas del cumplimiento de la ley deben respetar plazos para la utilización de los datos. Sin embargo, el controlador puede establecer distinciones para el tratamiento dependiendo del sujeto procesal cuyos datos se traten, es decir, atendiendo a si se trata de un testigo, víctima, imputado, perito u otro.

El acta en revisión admite también el tratamiento de categorías especiales de datos, como podrían ser los sensibles, cuando el uso en cuestión está expresamente autorizado por la ley, cuando el uso es de vital importancia para su titular o para cualquier otra persona natural y cuando los datos en comento han sido manifiestamente echo públicos por parte de su titular.

Un punto a destacar del instrumento en análisis es que regula de manera explícita el tratamiento automatizado de los datos personales en el contexto descrito, a saber, por parte de las autoridades encargadas del cumplimiento normativo para prevenir, detectar y procesar ofensas y para ejecutar sanciones, factor de suma relevancia considerando que Estonia se encuentra ad-portas de una marcha blanca para la aplicación automatizada de justicia.

En este sentido, la primera mención del acápite vigésimo primero es la prohibición explícita de cualquier decisión basada únicamente en un procesamiento automatizado de datos que pueda perjudicar a su titular o tener cualquier efecto significativo sobre su persona; prohibición que se matiza a continuación al añadir que tal decisión puede tomarse cuando la ley lo permita previendo medidas apropiadas para proteger los derechos, libertades e intereses legítimos del interesado.

Con todo, el sujeto afectado tiene derecho a objetar las decisiones automatizadas referidas en el acápite anterior cuando estas afecten sus intereses legítimos, con lo que se consagra el derecho de impugnación dentro del ámbito judicial estonio.

La norma va más allá y dispone que las decisiones automatizadas que pudieran adoptarse de conformidad con lo anterior, en todo caso, no pueden basarse en datos de categorías especiales, salvo que se apliquen medidas adecuadas para proteger los derechos, libertades e intereses legítimos de sus titulares, y que está especialmente prohibido basar estas decisiones en los resultados de perfilamientos de personas derivados de su discriminación a partir de categorías especiales de datos personales.

De esta manera, la regulación sobre la toma de decisiones automatizadas sobre personas naturales en el marco de un proceso judicial no es realmente tajante y tiene como principal consideración la posibilidad de oponerse por parte del afectado y el resguardo permanente de sus derechos, libertades e intereses legítimos. De manera que, en principio, se permiten tales decisiones siempre que sean respetuosas de dichas consideraciones y entendiendo que están siempre sujetas a la posibilidad de ser objetadas y revisadas por no haber intervenido un ser humano en ellas o por haber afectado tales intereses del titular. Así, una diferencia sutil con la próxima legislación chilena que radica en la formulación, pero que no por ello carece de relevancia, es que de acuerdo con el proyecto de ley chileno, el titular siempre podrá oponerse a una decisión automatizada que lo perjudique pudiendo exigir la intervención humana en su revisión, mientras que la norma estonia parece matizar esta premisa al dar mayor cabida a este tipo de decisiones que, no obstante ser susceptibles de objeción, pueden ser revisadas tomando 'medidas adecuadas' para la preservación de los derechos, libertades e intereses legítimos de sus titulares, lo que no necesariamente implica la participación humana en la revisión.

En cuanto a los derechos de los titulares de la información que atraviesan procesos judiciales, se reiteran los derechos ARCO y se pone especial énfasis en los deberes de acceso e información, tanto activa como pasiva, que deben ser facilitados por el controlador para que los afectados conozcan y puedan ejercer a cabalidad sus derechos. No obstante, dicha obligación de información activa puede ser retrasada o restringida si se estima que su comunicación es capaz de obstaculizar la prevención, detección o el procesamiento de ofensas, la ejecución de sanciones, dañar los derechos y/o libertades de terceros, poner el riesgo la seguridad nacional el orden público o entorpecer la investigación en curso.

En el curso del tratamiento judicial de datos personales, el controlador de la información está sujeto a estrictos deberes de *compliance* respecto de los deberes impuestos por el acta en comento y, no conforme con ello, debe hacerse responsable y velar también por el cumplimiento de la normativa y principios por parte del procesador, indicándole las directrices de tratamiento adecuadas. Más aun, el controlador no podrá permitir el tratamiento de los datos por cualquier procesador, sino sólo por parte de aquellos que ofrezcan garantías suficientes de cumplimiento en atención al establecimiento de medidas organizativas adecuadas, debiendo recurrir los procesadora inadecuados a aquellos que sí cumplen con los estándares para que los asistan en el tratamiento de la información requerida para llevar

a término el juicio en cuestión. Es como si en Santiago se determinara que de los 30 Tribunales Civiles sólo 22 cumplen con los estándares para confiarles el tratamiento de los datos personales de los sujetos procesales, debiendo los 8 restantes pedir ayuda a los capacitados para completar su labor.

De hecho, lo que establece la normativa estonia es una cadena de responsabilidades en que existe un controlador de los datos que es el primer responsable de la información y que puede determinar a qué procesadores entregar los datos para su tratamiento bajo estrictas directrices de cumplimiento, de manera que el procesamiento de la información efectuado por el procesador bajo estos parámetros será siempre responsabilidad del controlador, pasando entonces la responsabilidad al propio procesador cuando incumpla o exceda las directrices dadas por el controlador. Asimismo, el procesador está facultado para permitir el tratamiento de los datos por parte de terceros, siempre bajo los parámetros que el primero determine, pasando a ser responsable de lo que el tercero hace con la información.

Este esquema exige, además, que tanto el controlador como la autoridad encargada de la aplicación de justicia que procesa los datos lleven un acucioso registro de las actividades de tratamiento aplicadas sobre los datos personales, la que como mínimo debe contener las actividades de recolección de los datos, su enmienda, lectura, divulgación, transmisión, combinación y borrado, incluyendo la adecuada identificación de todos quienes hubieran accedido o intervenido de cualquier modo la información, pudiendo añadirse otros ítems en caso de haberse llevado a cabo otro tipo de acción sobre ella, como pueden ser el perfilamiento o uso de perfiles, la transmisión de los datos a terceros países u organizaciones internacionales, las medidas de seguridad adicionales aplicadas sobre la información, etc. La Agencia de protección de los datos personales puede requerir el contenido de este registro, en cuyo caso tanto el controlador como el procesador deben estar en condiciones de facilitarlo.

Armonizando con el RGPD, esta "Acta de protección de datos personales" pone de relieve la importancia de realizar estudios de impacto cuando el tratamiento de la información puede poner en riesgo los derechos y/o libertades de las personas naturales, de manera que previo a la realización de alguna actividad de tratamiento, el controlador debe evaluar el riesgo que esta puede involucrar. Al momento de realizar este tipo de evaluación, se debe tener en consideración la descripción sistemática del tipo de procesamiento de información que se pretende y su propósito, la valoración tanto de la necesidad como de la proporcionalidad de este procedimiento, la ponderación de los riesgos involucrados para los derechos, libertades e intereses legítimos de los afectados y las medidas previstas para afrontar dichos riesgos.

La autoridad de protección de datos toma protagonismo bajo determinados supuestos que requieren de su aprobación para poder llevarse a cabo. Entre las materias que deben ser consultadas a la agencia por parte del controlador o del procesador previo a su actuación se encuentran:

- Casos en que el controlador y procesador requieran de la creación de un nuevo sistema de tratamiento de datos cuya evaluación de impacto arroje que existe un alto riesgo para los afectados a falta de adecuadas medidas de seguridad o cuando la naturaleza de esta forma de procesamiento de información conlleve un alto riesgo para los derechos y libertades de los titulares.

  Cuando de esta consulta la autoridad de control estime que la propuesta de tratamiento de datos violaría alguna de las disposiciones del Acta de protección de datos en revisión, esta deberá proveer de una comunicación por escrito al controlador o procesador que contenga guías y consejos sobre cómo cumplir adecuadamente con los elementos requeridos de *compliance*.
- Para revisar la conformidad de las prácticas de tratamiento de datos personales con los requisitos de procesamiento de información, para lo cual se debe entregar toda la información de interés a la agencia. Requerida la autoridad de control a este respecto, deberá dar respuesta con sus directivas dentro de seis semanas, prorrogables en un mes adicional cuando la complejidad del caso lo amerite.

Habida cuenta de la significación y trascendencia que reviste la actividad judicial dentro de la sociedad, esta Acta enfatiza el deber de cuidado para el tratamiento de datos personales efectuado por autoridades encargadas del cumplimiento de la ley, señalando que el especialista de protección de datos ha de ser experto tanto en la legislación atingente como en la práctica de la seguridad de la información, debiendo además cumplir con la entrega de información y cooperación para con la Agencia de Protección de Datos Personales.

Así como el especialista de protección de datos personales tiene el deber de informar a la autoridad de control acerca de las brechas de seguridad que pueda identificar en su labor, el controlador y procesador tienen igual obligación cuando advierten la inminencia de alguna forma de riesgo para los derechos y libertades de las personas naturales, debiendo dar cuenta pormenorizada de las características de estos riesgos, el tipo de información de que se trata, la cantidad involucrada, el detalle de las posibles consecuencias del caso y las medidas que estimen convenientes tomar para controlar o mitigar la situación. Si el riesgo referido parece alto, grave o no se avizoran medidas adecuadas para reestablecer su control, se debe notificar igualmente de esta circunstancia a los titulares de la información cuyos derechos y libertades pudieran verse afectados por esta brecha de seguridad. Tal notificación debe efectuarse en términos sencillos y comprehensibles.

Por último, este cuerpo normativo regula los casos y condiciones bajo los cuales se puede enviar información personal a terceros países o a organizaciones internacionales. En términos amplios, estas

causales apuntan a que la operación en cuestión pueda contribuir a la prevención, detección o procesamiento de ofensas o a la ejecución de sanciones, manteniendo siempre el adecuado resguardo de los derechos libertades e intereses legítimos de os titulares de la información.

Los puntos revisados hasta aquí de la normativa estonia dan cuenta de un trabajo específico que apunta a regular de manera adecuada y fiel a las garantías de las personas el correcto uso de la información personal dentro de los procesos judiciales o de cumplimiento de ley, lo que constituye un ámbito sensible de la aplicación de sistemas de análisis de información y de suma relevancia para las sociedades. Esto ocurre en los términos expuestos en un país que se ha caracterizado los últimos 15 años por su inventiva y capacidad de innovación en la tecnologización del Estado y la digitalización de su ciudadanía.

Así, Estonia, como punta de lanza en la implementación de jueces robot y, en general de la toma de decisiones automatizadas dentro de los sistemas de aplicación de justicia, nos entrega los primeros parámetros concretos de regulación que son susceptibles de evaluación empírica para comenzar a proyectar su ámbito de aplicación futura en nuestro país.

El próximo capítulo abordará el rol del nuevo derecho a la impugnación que será añadido a la normativa chilena y cómo este, junto al esquema de recursos procesales vigente en el país, perfilan los ámbitos y medidas de aplicación posibles en el mediano plazo para las decisiones judiciales automatizadas.

CAPÍTULO III: El nuevo Derecho de Impugnación. Necesidades procesales especiales y evaluación de su compatibilidad con la aplicación de decisiones judiciales automatizadas.

Cómo vimos en el capítulo anterior, el derecho de impugnación constituye una de las novedades que se está imprimiendo a los catálogos de derechos de los titulares de datos personales en el RGPD y en el proyecto de ley que tiene el propósito de actualizar la ley 19.628 en Chile.

Ya desde la Directiva 95/46/CE de 1995, la Unión Europea contemplaba la prohibición de tomar decisiones con efectos jurídicos que se basaran únicamente en un tratamiento automatizado de datos. El RGPD reafirma este derecho en su artículo 22 dando al interesado la posibilidad de "no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar", lo que conlleva para el responsable del tratamiento de datos la obligación de garantizar mecanismos de notificación y ejercicio de este derecho, vale decir, facilitar la información relevante para el titular y establecer mecanismos que le permitan conocer cómo se ha tomado una decisión que lo perjudica, generando, a su vez, sistemas que den un procesamiento ágil a su solicitud de revisar de tal decisión. Estos sistemas tienen que contar indefectiblemente con la participación de una persona que revise y pondere la forma en que fue tomada la decisión cuestionada y las consecuencias que aquella supone para el interesado.

Si, bajo la legislación actual, se intentara aplicar en Chile este derecho, el escenario más probable sería el de las compañías ignorando las solicitudes de sus usuarios, cortando llamadas telefónicas y señalando que ellos no contemplan tales prácticas. Por otro lado, tendríamos al SERNAC intentando una mediación fútil entre consumidores y empresas, pero sin la potestad de sancionar o establecer directivas que pudiesen motivar un cambio en el comportamiento de las compañías que las hiciera ceñirse más fielmente a la ley. Es por ello que la adición de nuevas garantías conlleva la necesidad ineludible de consolidar una institucionalidad capaz de proteger a los abonados y de sancionar a las entidades que vulneren sus derechos. Pero, además, dicha institucionalidad debe establecer mecanismos sencillos, veloces y de bajo costo que aseguren a los ciudadanos la posibilidad de acceder a la justicia y hacer valer sus derechos.

Por lo pronto, el proyecto de ley que busca modificar la ley 19.628 incorpora el derecho a la impugnación en su artículo 8° bis como una modalidad especial del derecho de oposición contenido en

el artículo 8° del mismo proyecto.[7] De hecho, estaría recibiendo el nombre de "Derecho de oposición a valoraciones personales automatizadas". Así, el derecho de oposición a secas sería aplicable de manera genérica a los casos en que el responsable del tratamiento realice operaciones que conlleven una afectación a los derechos y libertades fundamentales de los titulares, cuando sólo tenga por objeto el marketing directo de bienes, productos o servicios o cuando los datos se hubieran obtenido de fuentes de acceso público no existiendo otro fundamento legal para su tratamiento. En cambio, el derecho de impugnación, u oposición a valoraciones personales automatizadas, se podría ejercer cuando el tratamiento de la información personal se lleve a cabo únicamente por medio de sistemas automatizados, es decir, sin intervención humana, y su decisión concierna al titular. No obstante, el titular no podrá ejercer este derecho si ha consentido previa y expresamente esta forma de tratamiento, cuando la ley disponga que el tratamiento automatizado es válido y cuando fuera necesario para ejecutar un contrato celebrado entre el titular y el responsable.

En otras palabras, el derecho de oposición está pensado en términos amplios para evitar los usos lesivos de los datos personales, siendo el derecho de impugnación una hipótesis mucho más restrictiva que se orienta en concreto al tratamiento automatizado de datos que puede generar decisiones y/o consecuencias gravosas para el titular. Sin perjuicio de ello, cabe recalcar que en la actualidad existe un creciente tratamiento de información realizado a través de sistemas automatizados, circunstancia que realza la importancia de este derecho y genera la necesidad de mantener estructuras para su resguardo que contemplen la intervención humana en el proceso y una adecuada trazabilidad de las distintas etapas del tratamiento de los datos.

Pero en términos concretos ¿cómo se garantiza este derecho?, ¿Cómo podría ejercerse?

Dado que en Chile no contamos aún con respuestas ideadas específicamente para este asunto, volveremos a las soluciones que se han dado en la Unión Europea para evaluar su aplicación en Chile. Esto teniendo en cuenta que la mayor parte del proyecto de ley que se encuentra en tramitación ha tenido como base los estándares generados por el RGPD.

Lo primero que llama la atención del caso europeo es la interpretación que hizo el Grupo de Trabajo del artículo 29 sobre este derecho. En sus Directrices sobre decisiones individuales automatizadas y elaboración de perfiles, el órgano consultor determinó que la interpretación correcta de este derecho supone que, en tanto derecho, no sólo debe aplicarse cuando el afectado lo invoca en forma activa, pues se trata de una "prohibición general de las decisiones basadas únicamente en el tratamiento

[7] La doctrina ha discutido si el derecho de impugnación corresponde a una modalidad del derecho de oposición o si tiene el carácter de un derecho independiente. Sin embargo, este trabajo no ahondará en tal discusión y nos limitaremos al hecho de que el legislador chileno lo ha tratado geográfica y explícitamente como una forma del derecho de oposición.

automatizado", pudiéndose omitir este deber sólo para los casos enumerados en el artículo 22 del RGPD, y añaden que interpretar este artículo como una prohibición general en lugar de un derecho que debe invocarse "significa que las personas están protegidas automáticamente frente a las posibles consecuencias que pueda tener este tipo de tratamiento" (Grupo de Trabajo sobre Protección de Datos del Artículo 29, 2018).

En el mismo trabajo se establece que las medidas de protección que obligatoriamente se deben adoptar para custodiar este derecho son:

a) Cumplimiento del derecho de información, debiéndose notificar en particular los aspectos significativos sobre la lógica aplicada, así como la importancia y las consecuencias previstas para el interesado.
b) Aseguramiento de la posibilidad de obtener intervención humana en el proceso, esto es, asegurar que la supervisión humana de las decisiones finales sea significativa y no una mera formalidad. Quien supervisa este último resultado debe ser una persona autorizada y competente para modificar las decisiones.
c) Derecho a impugnar la decisión automatizada.
d) Realización de una Evaluación de Impacto relativa a la protección de datos (EIPD) para aquellos casos en que el tratamiento conlleve un riesgo elevado para los interesados. Esta EIPD debe identificar los grados de participación humana que ocurren en el proceso y en qué puntos toman decisiones.

Respecto de este listado de medidas necesarias para un adecuado resguardo del derecho a impugnar decisiones automatizadas, parece factible la pronta implementación en Chile de las letras a) y c), toda vez que el proyecto de ley que se encuentra en tramitación contempla como requisito del tratamiento, el resguardo de los derechos de información e impugnación. No obstante, vale la pena destacar los adjetivos acompañados al requisito de informar, ya que, de acuerdo con el legislador europeo, la información a entregar al titular debe incluir los aspectos significativos de la lógica que se aplica sobre los datos, así como su importancia y las consecuencias previsibles para el interesado, aspectos que no se encuentran hoy explicitados para Chile, pero que se podrían incorporar al futuro reglamento de esta ley. Más aun, en el acápite sobre recomendación de buenas prácticas, esta Directiva sugiere que la etapa de información para el titular debiera además contemplar una explicación de las categorías de datos a utilizar, el por qué, de la necesidad de dichas categorías, la forma de elaboración de perfiles, los motivos que justifican que dicho perfil sea relevante para el fin perseguido y cómo puede producir efectos para el titular, pudiéndose tomar en cuenta la opinión de los titulares y facilitando su acceso a tales perfiles para que puedan conocer el proceso y corregir las inexactitudes.

De la misma enumeración, parecen ser más lejanas las letras b) y d), ya que si bien el proyecto de ley contempla el derecho a exigir la intervención humana en las decisiones automatizadas que puedan tener efectos significativos sobre una persona, no resulta igual de probable que la interpretación de dicha disposición vaya a resultar tan exigente como la europea que, como veíamos, ha comprendido el término "derecho" como una prohibición general de la toma de decisiones automatizadas sin intervención humana. Por otro lado, las Evaluaciones de Impacto no se contemplan en el proyecto de ley, de modo que, cuando mucho, podrían instaurarse como una buena práctica para las entidades que pretendan dedicarse al tratamiento masivo de datos personales. Asimismo, un futuro reglamento podría llegar a requerirla para determinadas prácticas, o su desarrollo podría derivar en una mayor velocidad para los análisis de cumplimiento de las entidades tratantes, o bien se podría otorgar una presunción de cumplimiento para quienes lleven a cabo estudios previos en esta materia, todo lo cual requeriría de la dictación de dicho reglamento y/o del pronunciamiento de la autoridad de protección.

Ya que, en la actualidad, la toma de decisiones se sustenta cada vez más en el tratamiento de datos, parece necesario reevaluar el procedimiento que se lleva a cabo para asegurar la protección de los derechos de los titulares sobre su información. Veíamos que el recurso de *Habeas Data* ha demostrado ser inútil para este propósito en vista de las dificultades que reviste para el usuario, tanto en efectividad, tardanza y en cuanto a sus costos asociados. No parece razonable para un individuo el tener que recurrir a la contratación de un abogado, iniciar un extenso juicio, pagar una notificación y eventualmente a un receptor en la etapa de rendición de pruebas sólo para lograr que una compañía transparente sus datos, deje de llamarlo cuando resulta molesto o reevalúe su decisión de negarle un crédito basada únicamente en el tratamiento automatizado de la información contenida en sus bases de datos.

Asimismo, resulta crucial generar condiciones, tanto normativas como educativas, que garanticen mayor proactividad por parte de las entidades tratantes de datos y un mayor grado de orientación y fiscalización que pueda traducirse en sanciones significativas capaces de influir en la toma de decisiones de los particulares.

En concreto, la Unión Europea ha optado por aplicar el mismo procedimiento para resguardar cualquiera de los derechos ARCOPI. Si bien dicho procedimiento presenta una gran similitud con el recurso de Habeas Data chileno, se logra una efectividad infinitamente superior dado que establece una competencia prioritaria en las Autoridades de Control para conocer las reclamaciones sobre vulneraciones al Reglamento y sobre materias de protección de datos, siendo secundario el rol de los Tribunales ordinarios, sin perjuicio de las acciones judiciales que les corresponda conocer. Esta estructura conlleva una mayor celeridad y una revisión mucho más especializada de los casos, además de condenas significativas para las entidades infractoras de la norma.

Tal como en la normativa chilena actual, para el RGPD los procedimientos destinados a proteger los derechos ARCOPI comienzan dirigiendo una comunicación directa a la entidad responsable de los datos a que refiere la consulta o vulneración. A continuación, el responsable tiene un mes, prorrogable, para dar respuesta a dicha comunicación. En caso de que no se efectúe la contestación dentro de plazo o si esta no resulta satisfactoria, el interesado puede recurrir mediante un reclamo a la Autoridad de Control o ejercer acciones judiciales o administrativas, según corresponda.

El Reclamo se interpone ante la Autoridad de Control, quedando ésta obligada a informar al reclamante sobre el curso y resultado de su acción, así como de proveerle información acerca de su posibilidad de acceso a la tutela judicial que el Reglamento garantiza en sus artículos 78 y 79.

El hecho de asegurar una tutela judicial efectiva para concurrir ante los Tribunales a todos quienes se muestren interesados en resguardar estos derechos constituye un salto enorme en las posibilidades de acceso a la justicia que debiese ser incorporado en Chile para que todos los afectados por acciones lesivas en cuanto al tratamiento de su información tuviesen una oportunidad real de hacer valer sus derechos.

En todo caso, esta tutela judicial no concurre en la etapa de revisión de la reclamación que se efectúa ante la Autoridad de Control, en tanto se trata de una instancia administrativa que tiene por objeto entregar una resolución veloz del conflicto y de sancionar cuando proceda. Las hipótesis en que tiene lugar este aseguramiento de la tutela judicial son las siguientes:

- Contra la Autoridad de Control:
    - Cuando el interesado no vea satisfecho su interés con la decisión tomada por la Autoridad de Control respecto de su reclamación, esto es, siempre que no se haya aceptado íntegramente su reclamación.
    - Cuando la Autoridad de Control no dé curso a la reclamación o no informe acerca de su curso o resultado en el plazo de 3 meses.
- Contra un responsable o encargado del tratamiento:
    - Siempre que el interesado considere que los derechos que le otorga el RGPD han sido vulnerados en el marco de su tratamiento.

Para desarrollar sus funciones, tanto preventivas como investigativas, la Autoridad de Control está investida de una serie de poderes que incluyen la facultad de ordenar la entrega de información a los responsables de los datos, la realización de auditorías relativas a la protección de los datos personales, revisar las certificaciones que dan cuenta de la adopción de medidas de seguridad adecuadas para los tipos y formas de tratamiento de datos que realizan, notificar a los responsables o encargados de sus presuntas infracciones al Reglamento, acceder a todos los datos personales y a la información necesaria

para el ejercicio de sus funciones por medio del responsable o encargado del tratamiento y obtener acceso a todos los locales del responsable y encargado, incluyendo los equipos y medios que utilicen para el tratamiento de la información. Asimismo, la Autoridad de Control puede establecer sanciones que van desde una advertencia o apercibimiento hasta limitaciones temporales o definitivas al tratamiento de datos, ordenar rectificaciones o supresión de datos personales, suspender el flujo de datos hacia un destinatario foráneo, retirar certificaciones y forzar la respuesta a las solicitudes de particulares.

Cuando las sanciones dispuestas consisten en multas, la autoridad de Control debe propender que estas resulten efectivas, proporcionadas y disuasorias, de modo que, para su dictación, deben tenerse diversos elementos en consideración, a saber:

- La naturaleza, gravedad y duración de la infracción en relación con los alcances y propósitos del tratamiento llevado a cabo, así como el número de interesados, afectados y el nivel del daño causado.
- La intencionalidad o negligencia de la infracción.
- Las medidas tomadas para paliar el daño.
- El grado de responsabilidad del responsable de acuerdo con su grado de cumplimiento de las medidas técnicas u organizativas correspondientes.
- La reiteración de infracciones.
- El grado de cooperación.
- Las categorías de datos personales afectados.
- La circunstancia del responsable o encargado de haber notificado su infracción a la Autoridad de Control.
- El grado de cumplimiento de medidas anteriores impuestas por la autoridad.
- La adhesión a códigos de conducta y certificaciones.
- Otros factores que, se estime, puedan atenuar o agravar la infracción, quedando abierta la esfera de evaluación a un sistema de sana crítica.

En Chile el proyecto de ley establece una clara división entre las normas que regulan el tratamiento de datos personales desarrollado por organismos públicos y privados; división que en el caso europeo queda entregada a la determinación de cada uno de los Estados miembros en observancia de sus diversas estructuras administrativas, pero estableciéndose, en todo caso, el objetivo de conciliar el acceso público a la información oficial y a la reutilización de los datos personales con la debida protección de la información por parte de las instituciones de los Estados, conforme al RGPD.

Cuando entre en vigencia la nueva ley de protección de datos personales, Chile dejará en el pasado el recurso de Habeas Data, que se sustituirá por un procedimiento similar, pero que pretende ser más

eficaz gracias al protagonismo de la agencia de Protección de Datos Personales. Aunque existirá una distinción entre los procedimientos de reclamación desarrollados contra organismos de la administración pública, la generalidad de los procedimientos de reclamación de las garantías contempladas en este proyecto se ejercerá bajo la directriz de los artículos 11, 23, 41 y siguientes del nuevo texto legal, según los que el primer paso para cualquier proceso de reclamación consistirá en presentar una solicitud ante el responsable de tratamiento de datos. Esta solicitud deberá contener la correcta individualización del titular y de su representante legal, según corresponda, la indicación de su dirección o correo electrónico para poder notificarle el curso y resultado del proceso y la identificación de los datos personales o forma de tratamiento que motivan la presentación. Cuando el derecho invocado sea el de oposición, el titular deberá señalar la causal específica, debiendo justificar brevemente el caso cuando se trate de la causal de afectación de sus derechos y libertades personales.

Una vez presentado este requerimiento, el responsable deberá acusar su recibo y tendrá 15 días hábiles para pronunciarse a su respecto, comunicando su respuesta al domicilio o dirección de correo señalado por el requirente y almacenando los respaldos que demuestran la transmisión, recepción, fecha y contenido de esta contestación cuando se hiciere a través de otros medios electrónicos.

En caso de no acoger íntegramente la solicitud, el responsable deberá fundamentar su decisión y señalar al titular que tendrá 15 días hábiles para formular una reclamación ante la Agencia de Protección de Datos Personales. Del mismo modo, si cumplido el plazo, el responsable no se pronuncia sobre el caso, el titular tendrá 15 días hábiles para formular su reclamo ante la Agencia.

Tratándose del ejercicio de los derechos de rectificación, cancelación u oposición[8], el titular tendrá derecho a que el responsable bloquee temporalmente sus datos o la forma específica de tratamiento cuando justifique adecuadamente esta solicitud, existiendo un plazo de sólo dos días hábiles para que el responsable responda a este requerimiento, no pudiendo tratar los datos en cuestión mientras no se pronuncie sobre esta petición. En caso de no acoger la solicitud de bloqueo, el mismo responsable deberá dar aviso a la Agencia de Protección de Datos Personales dando cuenta de sus motivos, pudiendo el titular reclamar ante el mismo organismo conforme al procedimiento general del artículo 41.

El procedimiento administrativo de tutela de derechos comienza por medio de una reclamación escrita que debe presentarse dentro de 15 días contados desde la respuesta negativa del responsable de datos o desde el vencimiento de su plazo para responder. La reclamación debe señalar la decisión

[8] Respecto de este punto se deberá determinar si la forma de oposición del artículo 8° bis (oposición a valoraciones personales automatizadas, o impugnación) dará igualmente derecho a bloquear los datos del interesado mientras se resuelve la acción.

impugnada o el hecho de no haberse contestado dentro de plazo y acompañar todos los antecedentes en que se funda, indicando una dirección de correo electrónico para futuras notificaciones.

Luego, la Agencia de Protección de Datos Personales tendrá 10 días para determinar si se cumple con los antedichos requisitos formales, en cuyo caso, dará lugar a la tramitación. En caso contrario el organismo deberá fundamentar este rechazo y notificarlo al titular.

Una vez acogida a trámite la reclamación, la Agencia de Protección de Datos Personales deberá notificar al responsable de los datos que, igualmente, tendrá un plazo de 15 días para responder esta reclamación acompañando todos los antecedentes relativos al caso. Vencido este plazo, e independiente de si contestó o no, la autoridad de control evaluará la existencia de hechos pertinentes, sustanciales y controvertidos y, en la afirmativa, abrirá un término probatorio de 10 días en el que las partes podrán hacer valer todos los medios de prueba que estimen convenientes.

Si el responsable se allana a la reclamación, la agencia lo notificará al titular y posteriormente procederá a la aplicación de una sanción cuando corresponda y al archivo de los antecedentes.

Como ya se explicó, en caso de que la Agencia de Protección de Datos requiera de datos adicionales a los aportados por las partes para formar su convicción respecto del asunto que conoce, tendrá amplias facultades para solicitar antecedentes, suspender el tratamiento de los datos objeto de la reclamación tras oír los motivos del responsable y convocar a las partes a audiencia, pudiendo instarlas a alcanzar un acuerdo en tal oportunidad. Las opiniones que pudieran emitir los funcionarios durante el desarrollo de dicha audiencia no serán causal de inhabilidad para seguir conociendo del asunto. En caso de lograrse un acuerdo de las partes, la agencia procederá a archivar los antecedentes.

Con todo, este procedimiento no podrá extenderse por un período mayor a seis meses y deberá concluir con la dictación de una resolución fundada dictada por la agencia que señale los recursos administrativos y judiciales que procedan en su contra.

En los casos en que la resolución de la Agencia de Protección de Datos Personales no hubiera acogido a tramitación un reclamo, así como cuando el resultado final de este procedimiento no satisficiera los intereses de alguna de las partes, ésta tendrá derecho a impugnar la decisión en un plazo de 15 días contados desde su notificación.

En su título IV, el proyecto de ley en tramitación consagra que, como regla general, el tratamiento de datos personales efectuado por órganos públicos es lícito en la medida que se lleve a cabo para el cumplimiento de sus funciones, dentro del ámbito de sus competencias y de conformidad a la ley, actuando como responsables de los datos y no requiriendo del consentimiento de sus respectivos titulares para tales casos.

Para estos efectos, aplican las mismas normas y principios que para los particulares, sumados a los de coordinación, eficiencia, transparencia y publicidad, en el entendido de su función pública.

El principio de coordinación aparece como uno relevante en el contexto del tratamiento masivo de datos y sus segundos usos, pues, conforme al artículo 21 del proyecto, apunta a que los distintos organismos públicos logren un alto grado de interoperabilidad y coherencia interna que eviten contradicciones y reiteraciones en la información almacenada. Pero la interoperabilidad va más allá de las eventuales contradicciones, ya que supone la posibilidad de los distintos organismos de acceder a una base común de información que pueda ser utilizada para propósitos completamente diversos en relación con el ámbito de operación de cada uno de ellos, lo que lleva a "segundos usos" permanentes y sistemáticos de los datos personales que, naturalmente, se ven facilitados en tanto estas instituciones no requerirán de autorización para el tratamiento de tal información bajo las condiciones antedichas y para el cumplimiento de sus funciones. Y es aquí donde cobran una importancia gravitante los principios de transparencia y los mecanismos de acceso activo y pasivo a la información pública, así como la trazabilidad, el respeto irrestricto a las normas de protección de los datos por parte de la administración pública y la adopción de altísimos estándares de seguridad respecto de la información.

Cuando el tratamiento sea desarrollado por organismos públicos, los titulares sólo podrán ejercer, ante el mismo organismo, los derechos de acceso, rectificación y oposición – con lo que el derecho de impugnación debiera ser igualmente aplicable ante un órgano del Estado dada la ubicación que se le dio dentro del proyecto-, ampliándose las causales de la oposición a aquellos usos impropio de la información personal de conformidad a los fines antedichos para la administración pública.

Con todo, los organismos públicos podrán rechazar de plano estas reclamaciones cuando:

- Impidan o entorpezcan las funciones fiscalizadoras, investigativas o sancionatorias del organismo en cuestión.
- Afecten el deber de secreto establecido por la ley.

Las acciones destinadas a tutelar estos derechos en el marco del tratamiento de datos efectuados por la administración pública deberán interponerse ante el jefe superior del servicio y sólo se podrá recurrir a la Agencia de Protección de Datos Personales cuando el organismo público haya denegado expresa o tácitamente la solicitud, en cuyo caso, el procedimiento se desarrollará conforme a las normas del procedimiento administrativo de tutela de derechos establecido en el artículo 43, referido en las próximas líneas.

Como veíamos, tanto para los procedimientos de reclamación suscitados entre particulares o entre un titular de datos y un órgano de la administración pública, cuando la resolución dictada por la Agencia

de Protección de Datos Personales cause agravio a alguna de las partes, estas tendrán derecho a impugnarla deduciendo un reclamo de ilegalidad ante la Corte de Apelaciones del domicilio del reclamante dentro de los 15 días siguientes a la notificación de la resolución impugnada.

El reclamo de ilegalidad deberá presentarse por escrito señalando la resolución que se impugna, las normas que se estiman infringidas, la forma en que estas habrían sido infringidas y, cuando corresponda, las razones que expliquen el agravio, pudiendo la Corte de Apelaciones declarar inadmisible el reclamo cuando no se cumpla con estos requisitos. Cuando la Corte de Apelaciones estime que el acto impugnado pudiere generar un daño irreparable al recurrente, podrá dictar orden de no innovar.

Una vez recibida la reclamación y aceptada a tramitación, la Corte de Apelaciones deberá requerir un informe a la Agencia de Protección de Datos Personales, el que deberá despacharse en un plazo de 10 días. Evacuado el traslado del recurrente o teniéndose por evacuado en rebeldía, la Corte podrá abrir un término probatorio que se sujetará a las reglas de los incidentes reguladas en el Código de Procedimiento Civil.

Vencido el término probatorio, se ordenará traer los autos en relación, gozando la causa de preferencia para su vista.

El fallo de la Corte se deberá fundamentar indicando si hubo o no agravio, en cuyo caso ordenará la rectificación del acto impugnado y la dictación de una nueva resolución. Esto también se aplicará cuando la resolución impugnada sea de carácter sancionatorio, pudiéndose confirmar o revocar, establecer o desechar la comisión de la infracción en cuestión.

Aunque, por desgracia, la nueva normativa chilena prescindirá de la garantía de tutela judicial establecida en el RGPD, es evidente la simplificación del proceso de reclamación que, una vez promulgado el proyecto, permitirá a cualquier titular de datos personales ejercer sus derechos y reclamar sus garantías ante un órgano especializado que deberá dar una respuesta veloz y eficaz al asunto, pudiendo establecer mecanismos de investigación intrusivos y sanciones significativas que, de aplicarse correctamente, constituirán un importante incentivo para que los responsables del tratamiento de los datos personales adopten medidas de resguardo y transparencia en sus futuros procesos.

Ya expuesto el procedimiento a seguir para el ejercicio del derecho de impugnación en Chile, cabe preguntarse por algunas de sus implicancias más allá de lo abstracto y teniendo en consideración la creciente aplicación de sistemas de decisiones automatizadas autónomos, es decir, de decisión propia y no mecánica, que se están aplicando en diversos lugares del mundo, desde la lejanía de Estonia con la marcha blanca de los jueces robot, hasta casos sumamente cercanos como la implementación del

software Prometea en Argentina y la Corte Interamericana de Derechos Humanos para elaborar proyectos de sentencia en casos determinados o de instrumentos diversos para el cálculo de la probabilidad de reincidencia de la población penal estadounidense que, naturalmente, incide en su posibilidad de acceder a beneficios penitenciarios.

La pregunta entonces tiene que ver con la factibilidad de instalar mecanismos de decisión automatizada y autónoma en sede judicial y con su ámbito de aplicación, en otros términos, la cuestión es cuál es la medida de aplicación posible de este tipo de decisiones en Chile bajo nuestro próximo sistema normativo y si es que serían necesarios mecanismos adicionales para la adecuada tutela de los derechos de los involucrados.

En este sentido, lo primero a destacar es que cuando hablamos de decisiones automatizadas en sede judicial, nos estamos refiriendo a una forma de tratamiento de datos ejercida por organismos públicos y para una finalidad específica, determinada de antemano y funcional a la administración del Estado, de manera que lo primero a despejar es que no sería posible aplicar este tipo de tecnologías sin antes atender al principio de legalidad administrativa y a la necesidad de que una ley establezca la posibilidad de llevar a cabo este tipo de tratamiento para un objetivo concreto. No obstante aquello, sería legítimo el tratamiento automatizado de la información personal para el cumplimiento de las funciones fiscalizadoras, investigativas o sancionatorias del organismo público, en la medida que se trate de sanciones administrativas por infracciones que sólo requieran la aplicación de un cálculo matemático.

Una vez que se cuente con dicha potestad legal, las normas generales a aplicar sobre este nuevo sistema de tratamiento serían las ya revisadas para el tratamiento de datos personales ejercidos por órganos de la administración pública y los subsecuentes procedimientos de reclamación revisados en este capítulo.

A este respecto, el proyecto de ley que modifica la ley 19.628 señala que son susceptibles de oposición todas las decisiones que conciernan a una persona en cuya determinación no hubieren participado seres humanos, no obstante lo cual se puede aprobar una ley que faculte a la institución para ello. Así, y salvo disposición legal en contrario, las decisiones judiciales automatizadas serían esencialmente revocables en la medida que no involucren un mecanismo de revisión humano previo a su dictación.

En este marco de revocabilidad es necesario tener siempre presente cuál es el tipo de asuntos en que típicamente podría errar un algoritmo y dónde el criterio humano podría ser sustantivo para la revisión de una decisión equívoca o mal ponderada. Destacan en este sentido elementos como los sesgos que probablemente podría padecer el sistema de evaluación, ya sea por sus condiciones de entrenamiento o por la sostenida obtención de conclusiones y aprendizaje que pudieran estar condicionadas por algún

parámetro previo al análisis y que deriven en una forma discriminatoria, así como también el elemento de opacidad del programa, es decir, el desconocimiento por parte de operadores y juristas acerca de cómo examina y resuelve el algoritmo. Esta falta de comprensión del criterio aplicado por la máquina dificulta seriamente la aseveración de su legalidad, puesto que no es clara la lógica detrás de una decisión y, por tanto, si esta se basa en pautas legales o no. Esto puede ocurrir ya porque el logaritmo utilizado no se hace público o bien porque la complejidad del análisis de este resulta muy elevada para quienes acompañan la actividad en cuestión. Sin embargo, esta transparencia debe compatibilizarse con las necesidades de seguridad del sistema informático del que se trate.

Sin perjuicio de lo anterior, el escenario más probable para la utilización de este tipo de herramientas en la aplicación de justicia es que el programa sea de conocimiento público o que al menos sea auditable, ya que el Estado debe cumplir con importantes estándares de transparencia y, entre los pilares del debido proceso se encuentran tanto la igualdad ante la ley, el racional y justo proceso, como también la obligación de argumentar las razones de una determinada resolución. Así, igualdad y racionalidad pueden ponerse en tela de juicio cuando no se conoce a cabalidad el esquema de reflexión propio del mecanismo bajo el cual se pretende resolver, y lo propio ocurre con la argumentación de los motivos de una decisión si, en efecto, se desconoce el fundamento de aquella. Tal barrera vuelve imprescindible una reserva de raciocinio humano detrás de las resoluciones que pueda adoptar una máquina, lo que se consagra con el derecho a la impugnación y los recursos fijados para su ejercicio.

Con todo, para los organismos públicos no basta con garantizar una instancia de apelación con participación humana, sino también velar por la transparencia y legitimidad del proceso y sus instituciones, de manera que no puede sino ser conocido el sistema de análisis a utilizar sobre la información. Esta necesidad, por cierto, transciende al conocimiento público del código del programa, puesto que también requiere que su funcionamiento sea puesto en conocimiento de la ciudadanía en términos claros y comprensibles, esto es, cuál es la finalidad del organismo, para qué se usa el algoritmo en comento, cómo funciona, cómo razona y de qué manera dicho funcionamiento es compatible y coadyuva al cumplimiento del deber público.[9]

Un ejemplo de lo anterior lo encontramos en el registro de algoritmos que utilizan inteligencia artificial que se está trabajando en Ámsterdam, donde se permite a los usuarios conocer todos los sistemas con tales características que son aplicados dentro de la ciudad, con una explicación sobre su

[9] Cabe destacar que este punto puede desatar conflictos con los derechos de propiedad intelectual que existan sobre los mismos cuando los autores o dueños del programa no quieran darlo a conocer. Es un punto que deberá ser ponderado por la autoridad pública en términos de si resulta más conveniente licitar la creación de sistemas *ad hoc*, utilizar mayoritariamente herramientas de código abierto o celebrar contratos estrictos con privados que establezcan las responsabilidades del caso y las correspondientes obligaciones de confidencialidad.

función, las bases de datos que utilizan, cómo y para qué procesan la información, entre otros aspectos. Este compendio, alojado en un sitio web abierto, todavía se encuentra en construcción, pero constituye una excelente iniciativa de transparencia activa en términos del derecho de información que corresponde a todos los titulares de información cuyos datos son objeto de tratamiento con miras a la tecnologización e interoperabilidad de la ciudad. (Chief Science Office, Gemeente Amsterdam, 2022).

Junto con ello, es sustancial el establecimiento de una clara distribución de responsabilidades bajo las que se pueda determinar en todo momento la o las personas que deben responder por una forma de tratamiento concreta y por la seguridad de la información en cada etapa del proceso, de manera que si llega a ser necesario el tratamiento de los datos por parte de un tercero, este sea reglado, limitado al fin previamente especificado y siempre exista certeza acerca de la persona sobre la que recaen las responsabilidades del caso, tal como ya ocurre en Estonia.

El 8 de abril de 2019, la Comisión Europea emitió una Comunicación referida a la generación de confianza en los sistemas de inteligencia artificial centrando su funcionamiento en el ser humano. En el documento la Comisión elabora un listado de siete requisitos para hacerla fiable que resumen bastante bien los aspectos tratados hasta aquí, a saber: (Dirección General de Redes de Comunicación, Contenido y Tecnologías de la Comisión Europea, 2019)

- **Intervención y supervisión humana competente,** teniendo como foco los derechos fundamentales de las personas y el bienestar global de los usuarios. Para ello deben ser aplicables medidas de control y adaptación de los sistemas.
- **Solidez y seguridad técnica,** esto refiere a aspectos como la coherencia interna de los programas, su capacidad para resolver errores, atender contingencias y responder ante ataques externos, así como para reflejar el grado de acierto de sus resultados y poder reproducirlos.
- **Privacidad y gestión de datos en todas las fases del sistema.** Para ello es útil idear sistemas que tengan como prioridad la protección de la privacidad y que, por tanto, se estructuren de manera consecuente desde su planteamiento. A esto se le ha llamado privacidad por defecto o privacidad desde el diseño.
- **Transparencia,** destacando en este punto tanto la trazabilidad de la información y de sus tratamientos, como la posibilidad de explicar las decisiones adoptadas.
- **Diversidad, no discriminación y equidad,** debiéndose prever eventuales sesgos o las deficiencias del modelo de gobernanza aplicado.

- **Bienestar social y medioambiental**, manteniendo cuidados sobre el impacto que puede causar la utilización de estos sistemas sobre seres humanos, seres sensibles, el medioambiente y la sostenibilidad en orden a la preservación de las generaciones futuras.
- **Rendición de cuentas** sobre los resultados de los programas que utilizan inteligencia artificial, tanto antes como después de su implementación, y el establecimiento claro de responsabilidades a lo largo del tratamiento de la información. Para ello son fundamentales las evaluaciones de impacto y las auditorías internas y externas.

Bajo un esquema respetuoso de estos principios, con miras la próxima normativa chilena y teniendo en consideración el grado de avance que poseen en la actualidad los *softwares* de apoyo a la administración de justicia, no parece razonable esperar que Chile avance prontamente en la implementación de jueces robot como Estonia, ni tampoco en sistemas que tomen las decisiones que hoy corresponden a un juez. Sin embargo, existe una esfera adecuada para su utilización, entendiendo que es posible apoyar el trabajo y la capacidad de decisión humana en tecnologías capaces de procesar más información y a mayor velocidad, así como también que puedan identificar patrones, sistematizar decisiones anteriores y advertir una gran cantidad de elementos que en la revisión llevada causa por causa por una persona son fáciles de perder. Así, toma relevancia el uso que se puede dar a estos mecanismos para apoyar las funciones encargadas a seres humanos y que requieren de la revisión de mucha información para su resolución, como puede ser la búsqueda y comparación de sentencias o doctrina afines a un caso, la ponderación de determinados riesgos, la identificación de patrones de conducta, la revisión de las formalidades requeridas o exámenes de forma, los sistemas de predicción de comportamiento, ya sea de decisiones de organismos jurisdiccionales como de cumplimiento de programas, reincidencia, entre muchos otros. Ahora bien, el uso de cualquiera de estos mecanismos para la adopción de una decisión respecto de una persona debiera ser un antecedente de carácter no vinculante a revisar por el responsable previo a su dictación oficial. En su defecto, la no revisión previa por parte de una persona natural haría impugnable la decisión siempre que cause cualquier forma de menoscabo al afectado.

En definitiva, este rol de apoyo a la actividad jurisdiccional supondría la existencia de un responsable que sea una persona natural competente, capaz de comprender el sistema que se aplica, sus motivos y de ponderar si la propuesta decisoria entregada por un programa se adecua a las normas aplicables y es respetuosa de los derechos y libertades de las personas. De tal manera, la falta de una instancia de revisión humana previo a la dictación de una resolución la volvería esencialmente revocable, como veíamos con antelación, siendo susceptible del recurso de impugnación ya revisado.

¿Qué rol juega entonces el derecho a la impugnación y su ejercicio frente a la eventual toma de decisiones judiciales automatizadas?

La Constitución Política de la República de Chile establece en su artículo 19 n°3 inciso 6° que "toda sentencia de un órgano que ejerza jurisdicción debe fundarse en un proceso previo legalmente tramitado. Corresponderá al legislador establecer siempre las garantías de un procedimiento y una investigación racionales y justos", con lo que nuestro sistema jurídico adopta la garantía fundamental del debido proceso que se ha visto complementada gracias a la suscripción de tratados internacionales y a la doctrina. Entre los puntos a destacar para lo que interesa a este trabajo, el artículo 25 de la Convención Americana sobre Derechos Humanos establece que "toda persona tiene derecho a un recurso sencillo y rápido o a cualquier otro recurso efectivo ante los jueces o tribunales competentes, que la ampare contra actos que violen sus derechos fundamentales reconocidos por la Constitución, la ley o la presente Convención, aun cuando tal violación sea cometida por personas que actúen en ejercicio de sus funciones oficiales".

Así, la impugnación sería un mecanismo propio del debido proceso en tanto manifestación del derecho al recurso, que tiene por objeto el restablecimiento, en forma rápida y sencilla, de un derecho o garantía que se ha visto vulnerado por la decisión automatizada emanada de un privado o bien de un órgano de la administración del Estado.

En concreto, el ejercicio del derecho de impugnación tendría dos instancias, la primera, al igual que el recurso de reposición, ante la propia entidad de la que emana la decisión lesiva con el objeto de que esta misma corrija su actuación, y la segunda, en caso de no ser satisfecha la pretensión anterior, consistiría en la interposición de un recurso ante el superior jerárquico, impugnando o contrariando la decisión insatisfactoria de la entidad con el objeto de reestablecer el derecho afectado por ella, tratándose entonces de un recurso ordinario de enmienda, homologable a la apelación, que si bien no elimina la decisión anterior por sus vicios inherentes, lo que hace es exigir su corrección o cambio de criterio en atención a la transgresión de derechos o libertades expuestos al momento de la reclamación.

Con todo, y aun tratándose de una forma de materialización del debido proceso, las hipótesis de ejercicio de este derecho no son absolutas y es posible inhibir su ejercicio cuando previo a la dictación de la decisión lesiva se ha cumplido con alguna de las excepciones habilitantes para la toma de decisiones automatizadas. Esto es, cuando la decisión automatizada sea necesaria para la celebración o ejecución de un contrato entre el titular y el responsable, cuando el titular haya consentido previa y expresamente que la decisión en cuestión pueda ser adoptada por un sistema automatizado o cuando exista una disposición legal que faculte al responsable de los datos a tomar determinadas decisiones en base a datos personales por medio de mecanismos automatizados, añadiéndose para los órganos de la administración

pública las hipótesis de cumplimiento de las funciones fiscalizadoras, investigativas o sancionatorias del organismo público y el deber de secreto o reserva establecido en la ley.

Vista esta formulación, y en abstracto, sí sería posible establecer legalmente la implementación decisiones judiciales automatizadas o de jueces robot sin que hubiera cabida a un recurso impugnatorio por el sólo hecho de no mediar participación humana en la toma de las decisiones judiciales, de manera que los recursos aplicables a cada caso serían los propios de cada procedimiento, tal como si estos fueran fallados por seres humanos. Ahora, la viabilidad de esta medida en todo caso dependería de que los sistemas en cuestión fueran capaces de preservar las demás garantías fundamentales, el debido proceso, los derechos y libertades de las personas que se vieran sometidas a los mismos, así como también de dar cumplimiento a todas las demás disposiciones de la ley de protección de los datos personales, por lo que restarían numerosos aspectos sustantivos y técnicos a evaluar.

Un escenario menos distante, entonces, sería el del uso de sistemas automatizados para la sugerencia de decisiones no vinculantes como apoyo a la actividad judicial con cuidado de las garantías fundamentales de los titulares de la información y, bajo el entendido de que, en su rol de sugerencias de decisión no vinculantes, estas sí serían susceptibles de impugnar en caso de no mediar participación humana en la decisión final, cuando la participación humana no fuera competente para la toma de la decisión e, igualmente, cuando la participación humana ocurriera como una mera formalidad para cumplir con la norma.

Sin perjuicio de la posibilidad de limitar el ejercicio del derecho de impugnación bajo los supuestos antedichos, y especialmente por disponerlo así la ley, en caso de existir una duda fundada acerca de si cabe o no la interposición del recurso en comento para contravenir la decisión adoptada por un organismo público, como podría ocurrir si se tomaran decisiones automatizadas en sede judicial, cabe destacar la conclusión del fallo pronunciado en agosto de 2021 por la Tercera Sala de la Corte Suprema en la causa N°143.992-2020 que opta por una interpretación pro recursiva cuando no existe claridad acerca de la impugnabilidad de actos administrativos.

En este sentido, la sentencia sostiene en su considerando cuarto que esta interpretación "…debe preferirse, por ser acorde al derecho al recurso consagrado como un mandato con toda su fuerza en el artículo 8.2 letra h) de la Convención Americana de Derechos Humanos que dispone el derecho al recurso judicial ante un tribunal superior, así como lo normado en el artículo 2.3 letra a) del Pacto Internacional de Derechos Civiles y Políticos que reconoce el derecho a una acción efectiva ante los tribunales a las personas cuyos derechos y libertades hayan sido violados", lo que se complementa en el considerando sexto al afirmar que "esta Corte considera que no se puede restringir a la revisión de una decisión de un organismo administrativo, cuando de la propia ley es posible desprender una interpretación en favor de

la procedencia de la apelación…" – que, para el caso, sería homologable a la reclamación judicial de los derechos ARCOP-.

Antes de concluir este capítulo, merece la pena abordar un punto potencialmente conflictivo respecto del considerando sexto para el caso de la impugnación de decisiones judiciales automatizadas y es el hecho de que tales decisiones agraviantes ocurrirían en el marco de la actividad judicial, por lo que podría resultar contraintuitivo judicializar una decisión automatizada lesiva pronunciada justamente por un tribunal. Sin embargo, la hipótesis supone que si dentro de la tramitación de un juicio el tribunal llega a tomar una decisión automatizada que vulnere los derechos de un involucrado y sin participación humana, el interesado tendría la posibilidad de representar específicamente el resultado de la decisión al propio organismo pidiendo su modificación, debiendo este dar una respuesta dentro de plazo que, en caso de ser negativa o insatisfactoria, permitiría al titular recurrir a la Agencia de Protección de Datos y posteriormente a la Corte de Apelaciones a fin de impugnar este acto. De manera que lo único que se tramitaría por vía paralela es la impugnación de la decisión automatizada y no los demás aspectos involucrados en el juicio originario. Para poder llevar a cabo todo este proceso es probable que sea necesario solicitar orden de no innovar al tribunal original hasta resolver el punto en conflicto, de lo contrario el juicio seguiría adelante teniendo como base una decisión viciada. Ya que este mecanismo podría servir simplemente para dilatar el juicio base, la concesión de la orden de no innovar debiera sujetarse a la significación de la decisión impugnada y los efectos que esta podría llegar a tener sobre el afectado que, en caso de no resultar irreversibles, permitiría continuar con la tramitación del juicio como si el recurso se conociera sólo con efecto devolutivo, pudiendo llegar a dejar sin efecto lo tramitado en el intertanto si finalmente se acogiera la reclamación impugnatoria de la decisión.

Bajo este esquema de principios y resguardos procesales, la postura de este trabajo es que resulta factible bajo el próximo modelo regulatorio la implementación de sistemas automatizados, tanto mecánicos como autónomos, para el apoyo de la actividad judicial, que sean capaces de resolver conflictos, ofrecer información y/o emitir decisiones no vinculantes que sirvan de base a la tarea de resolver casos de significancia jurídica encargados a jueces humanos.

CAPÍTULO IV: Desafíos Regulatorios Adicionales

En los capítulos anteriores hemos visto los importantes saltos que están dando las regulaciones de uso de datos personales, primero, gracias al impulso que ha dado la Unión Europea a la comunidad internacional en esta materia, los interesantes avances de Estonia que tienen al mundo expectante tanto de su ímpetu de innovación como de la efectividad de sus medidas, y, más concretamente, los cambios que se aproximan en el escenario chileno y que se encuentran a la espera de la promulgación de los proyectos de ley analizados para los ámbitos de la privacidad y el cibercrimen.

La creación de una autoridad de control que pueda supervisar, sancionar y educar en orden a lograr un esquema de tratamiento de datos personales respetuoso de los derechos de sus titulares, la facultad de fiscalizar, la exigencia de trazabilidad en las operaciones, la simplificación de los procesos y del acceso a la justicia para los titulares, los incentivos a la creación de códigos de conducta y a la realización de evaluaciones de impacto respecto de las eventuales esferas de afectación relacionadas con un sistema de tratamiento de datos personales, la homologación de los sistemas legislativos estatales que atienden fenómenos típicamente transnacionales, la colaboración internacional en el marco de las diligencias investigativas de delitos informáticos y la creación de la red 24/7 para facilitar la conservación de la información relevante y la realización de trámites urgentes son sólo algunos de los destacables elementos que traen consigo las regulaciones más modernas sobre los sistemas informáticos. Con estas herramientas ha sido posible abordar complejos casos contra gigantes informáticos como Facebook y Google, entre otros, y establecer restricciones ex ante para su funcionamiento en el mercado europeo. En cuanto a Chile, si bien el proyecto de ley de protección de datos personales lleva años con decreto de urgencia para su tramitación, podría tener por delante algunos meses más de discusión, por lo que resulta improbable que comience a aplicarse dentro de 2022.

Con todo, resulta que el derecho avanza mucho más lento que la ciencia y la tecnología, de modo que, incluso antes de su entrada en vigencia, estas normas ya parecen estar desactualizadas frente a una serie de fenómenos que no fueron previstos en ellas y sobre los que habrá que forzar sus parámetros para lograr soluciones razonables.

Entre los fenómenos que quedarían desprovistos de regulación propia podemos encontrar diversas situaciones que hemos visto numerosas veces como curiosidad o noticia en medios diversos. Destacamos entre ellos los siguientes casos:

1) Las afectaciones de la libre competencia sobre la privacidad:

El RGPD llevaba sólo unos meses en vigencia cuando evidenció su insuficiencia a la hora de abordar prácticas propias de otras disciplinas que tenían el potencial de afectar significativamente los derechos otorgados por este reglamento a los titulares de datos personales.

Así lo han evidenciado los diversos fallos que durante los últimos años han debido dictar las autoridades de control de la libre competencia objetando e impidiendo la compra de *startups*[10] por parte de gigantes de la información y tecnología.

En su fallo de 2019 contra Facebook respecto del uso de términos abusivos por parte de este último, el Bundeskartellamt[11], estimó que, si bien las leyes de protección de datos y las de competencia tenían finalidades diversas, ya no se podía excluir los asuntos de los datos personales del ámbito de la libre competencia, puesto que las decisiones tomadas por una empresa sobre la recopilación y uso de datos personales pueden tener implicancias económicas y sobre la competencia.

Por lo tanto, las normas de protección de datos podrían considerarse desde el punto de vista de la competencia cuando se trate de empresas controladoras que utilicen los datos como una entrada principal de sus productos o servicios, con lo que el RGPD ya no sería aplicable únicamente por parte de la autoridad de control de datos personales (Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate, 2019).

Al poco tiempo, numerosas autoridades de control de la competencia de diversos países comenzaron a pronunciarse sobre cuestiones de protección de datos personales y su eventual afectación a la competencia en el marco de negociaciones de adquisición de *startups*, como vimos en el intento de compra de Cornershop[12] por parte de Walmart que, si bien fue autorizada en Chile, no logró prosperar producto del bloqueo de la Comisión Federal de Competencia Económica (COFECE) en México. Los razonamientos de la FNE y la COFECE, aunque llegan a conclusiones opuestas, son útiles para comprender el tipo de afectaciones que el uso de datos personales puede llegar a producir en el campo de la competencia.

[10] Startup es el nombre con que se ha denominado a empresas emergentes e innovadoras que llevan poco tiempo en el mercado, pero que evidencian un enorme potencial de crecimiento.
[11] Autoridad de competencia alemana.
[12] Aplicación móvil producida en Chile que opera como intermediaria en la compra de alimentos, mercadería y otros productos que luego son entregados en la dirección entregada por el usuario.

A continuación, se exponen algunos de los elementos que ambas autoridades consideraron potencialmente riesgosos para el mercado (Adquisición decontrol sobre Delivery Technologies SpA por parte de Walmart Chile, 2019), (Versión pública de la resolución del expediente CNT-161-2018 , 2019):

- Al acceder a los clientes de Cornershop, Walmart podría conocer sus patrones de consumo, endeudamiento, ubicación, comercios y productos preferenciales, cantidad de compras y su frecuencia, entre otros datos de relevancia.
- Asimismo, podría llegar a conocer la forma en que se relaciona cada usuario con otras cadenas de supermercados, incluyendo sus estrategias de mercado, precios, promociones, calidad del servicio, entre otros.
- Los aspectos anteriores constituirían una adquisición de información estratégica de gran valor que podría repercutir en la modificación de sus propias estrategias de mercado en base al monitoreo permanente de la competencia y sus clientes respectivos, pudiendo llegar a generar publicidad altamente personalizada que explote a su favor las características de la relación del cliente con cada uno de los competidores.
- El control de Walmart sobre la plataforma de Cornershop podría derivar en un tratamiento privilegiado sobre sus propios productos en desmedro de los de la competencia, desviando la intención de compra de los usuarios.
- En esta misma línea, Walmart podría atentar contra los competidores de Cornershop negándose a figurar en otras plataformas similares, lo que obstaculizaría significativamente el desarrollo del mercado para estas aplicaciones.
- De igual manera, Cornershop podría impedir la participación de los competidores de Walmart en la plataforma o diseñar ventajas y beneficios en su favor.

Todas las prácticas anticompetitivas descritas podrían haber llegado a producirse con una adquisición de estas características, lo que da cuenta, por un lado, de la importancia de abordar estos factores en la regulación y, por otro, del potencial de desarrollo de esta área.

Con el tiempo, las autoridades de control de la competencia han debido desarrollar este tipo de análisis en numerosos casos adicionales, entre ellos, y sólo por nombrar algunos, la adquisición de Cornershop por parte de UBER[13], la evaluación de la situación de abuso de posición dominante de MercadoLibre en Uruguay, la revisión de la fusión entre AT&T y Time Warner en Chile, la compra de Giphy por parte de Facebook, entre muchos más.

[13] Que sí logró la aprobación tanto en Chile como en México.

El significativo aumento de estos casos en los últimos años, el enorme impacto sobre los mercados que deriva de las grandes compañías que normalmente se involucran en estas operaciones y la perspectiva de que este tipo de operaciones se vuelvan cada vez más habituales, parece haber llevado a las autoridades a dar una primera respuesta considerablemente rápida frente a este escenario.

El 15 de diciembre de 2020, la Comisión Europea presentó su propuesta de reglamento sobre mercados disputables y equitativos en el sector digital (Comisión Europea, 2020) que tiene por objeto evitar las prácticas abusivas por parte de las grandes plataformas tecnológicas dentro del mercado digital. Con esta finalidad se plantea un cambio de enfoque que busca establecer mecanismos de control *ex-ante* que prevengan la consecución, reforzamiento o conservación de posiciones dominantes de mercado mediante prácticas abusivas.

Además, vale la pena destacar que el proyecto se centra en el rol de los denominados *"gatekeepers"*, es decir, aquellas plataformas que, debido a su enorme posicionamiento, se han convertido en canales de acceso inevitables para todos los demás emprendedores (Ferrer, 2020).

No se analizarán en este trabajo los pormenores de esta propuesta, pero sí se destaca su importancia como un paso significativo en la regulación de este fenómeno.

2) Materias de Bioética:

Conforme aumenta la tecnología y se complejiza la técnica, suelen aparecer cada vez más usos y aplicaciones que, en muchos casos, tienen orientaciones filantrópicas y buscan simplificar el desarrollo de la vida para quienes presentan algún tipo de déficit en el desarrollo de las habilidades que, en promedio, demanda la sociedad de las personas. Así, hemos podido celebrar la diversificación de herramientas computacionales que facilitan el estudio de programas o carreras universitarias para personas no videntes, el perfeccionamiento de los sistemas que funcionan con comandos de voz, la masificación y democratización de las prótesis gracias a las impresoras 3D y a la participación de cada vez más desarrolladores en su planificación y creación, que permite hallar una enorme variedad de plantillas que pueden ajustarse a las particularidades de las personas que las requieren.

Sin embargo, se han presentado otro tipo de situaciones en que se proveen dispositivos de apoyo destinados a suplir deficiencias determinadas, pero que, en lugar de consistir en un apoyo meramente mecánico o en sistemas externos que facilitan el acceso a la información, funcionan conectados directamente al cerebro de las personas, permitiendo la percepción artificial de estímulos que son procesados como datos y aprehendidos por el cerebro que, gracias a la traducción que hace el dispositivo,

es capaz de analizar estas enormes cantidades de información, de aprender y de lograr una progresiva mejora en el cumplimiento de la función que se trata de complementar.

Lo que sin duda es una gran victoria de la ciencia y una mejora sustantiva en la calidad de vida de quienes portan estos dispositivos, es a su vez un asunto polémico que ha despertado importantes debates en el campo de la bioética.

A la fecha ya son varias las personas que han instalado en sus cuerpos este tipo de dispositivos y han logrado desarrollar habilidades suprahumanas. Se les conoce como cyborgs o transhumanos por incorporar elementos inorgánicos al cuerpo y por trascender a las habilidades humanas, respectivamente. Así, es posible percibir colores más allá de nuestro espectro, como lo hace Neil Harbisson, quien originalmente sólo podía ver el mundo en escala de grises, pero que, gracias a la instalación de una antena que capta las ondas de los colores, ha sido capaz de escucharlos y procesarlos, pudiendo percibir incluso las gamas infrarroja y ultravioleta. No conforme con ello, se ha planteado la meta de extender todavía más este espectro para lograr percibir, por ejemplo, las ondas de microonda y los rayos X, entre otros y de incluir nuevos sentidos a su cuerpo (Harbisson, 2018). Asimismo, está Moon Rivas, quien implantó sensores en sus pies que le permiten percibir las vibraciones de la tierra gracias a su conexión con un sismógrafo online, con lo que puede sentir los temblores que se generan en lugares lejanos cada pocos minutos (CNN, 2018).

En este sentido, cabe destacar el hecho de que Neil Harbisson es el primer ser humano que ha sido reconocido como cyborg por un Estado, a saber, Reino Unido que, al aceptar que la antena instalada en su cabeza formaba parte de su persona, le otorgó oficialmente esta calidad especial.

El objetivo que se plantean los cyborg y quienes apoyan este movimiento, es que podamos diseñarnos a nosotros mismos, definiendo nuestros sentidos y habilidades a partir de la tecnología disponible, "ser tecnología" (Harbisson, 2018).

De esta manera, se genera un importante desafío ético, o bioético, en lo que dice relación con el uso de bases de datos masivas que no necesariamente se componen de información personal o sensible, pero cuyo uso puede tener importantes repercusiones en el desenvolvimiento de las sociedades y en el interrelacionamiento de sus miembros, toda vez que pueden entrar en disputa principios como las libertades personales y la competencia justa entre aquellos individuos que, con miras a un ámbito específico, han incrementado determinadas competencias en desmedro de aquellos que optan por mantener sus 5 sentidos básicos y el manejo tecnológico por fuera del cuerpo propio, volviendo difícil y en ocasiones hasta imposible una competencia equitativa entre unos y otros, circunstancia que sin lugar a dudas resulta potencialmente compleja en la evolución de una sociedad que tiene entre sus cimientos la competencia de sus miembros.

Otro importante desafío bioético que ya nos golpea la puerta, corresponde al rol que jugarán en un futuro próximo los neuroderechos, un planteamiento *sui generis* que se ha presentado como una inquietud razonable por parte de las comunidades médicas, científicas e informáticas ante los avances de disciplinas como las neurociencias y el potencial que estas abren al combinarse con las nuevas capacidades de procesamiento a que da lugar el desarrollo de la inteligencia artificial.

De un tiempo a esta parte, el entendimiento del comportamiento del cerebro humano y del funcionamiento neuronal se han incrementado a tal punto que en la actualidad es posible trazar mapas neuronales que dan cuenta de las estructuras y formas de pensamiento, así como de los mecanismos de procesamiento de información de nuestros cerebros, los que pueden ser aprehendidos y, hasta cierto punto, replicados por redes neuronales artificiales capaces de emular algunos de sus aspectos o de combinarse con las redes biológicas en orden a mejorar su funcionamiento respecto de ámbitos determinados, lo que nos devuelve a interrogantes como las que veíamos a propósito de los *cyborg* o aquellas que apuntan directamente al resguardo de la privacidad en una de sus esferas más íntimas, e incluso a la duda respecto de la individualidad de las decisiones, así como a las dificultades de determinar la culpa de un individuo que provoque algún tipo de daño derivado de una decisión o movimiento estimulado parcialmente por el componente externo o artificial de un sistema neurológico mixto (Siebert, 2019).

Frente a este escenario se ha abierto una discusión de carácter ético, jurídico y regulatorio que busca determinar los alcances socialmente adecuados para el desarrollo de esta empresa dentro de la sociedad humana contemporánea, y aunque todavía existe un carácter fuertemente especulativo a este respecto, podemos encontrar algunos lineamientos básicos que desde hace algunos años permiten perfilar lo que podría ser desarrollado como una primera política pública para abordar este desafío. En este sentido, destaca la publicación de Rafael Yuste junto a un conjunto de expertos en estas materias, quienes el año 2017 publicaron un artículo en la revista Nature dando cuenta de los que serían las prioridades éticas para las neurotecnologías y la Inteligencia Artificial, a saber, la privacidad mental, la identidad personal, el libre albedrío y la igualdad, vale decir, el acceso equitativo y la no discriminación en el acceso a las neurotecnologías (Yuste, Goering, & otros, 2017).

Tomando como base estas inquietudes y reflexiones, Chile ha tomado la iniciativa y busca convertirse en el primer país en establecer una normativa, por lo pronto preventiva, que pueda anticiparse a los usos y efectos de este tipo de tecnologías estableciendo un estatuto de derechos, límites y obligaciones antes de que los efectos de una utilización indiscriminada de estos sistemas puedan resultar lesivo para las personas y comunidades.

El proyecto de ley fue ingresado en 7 de octubre de 2020 por la Comisión de Desafíos del Futuro, Ciencia, Tecnología e Innovación y prontamente fue aprobado en general en la Cámara de origen, sin embargo, se encuentra aún en su segundo trámite constitucional en la Cámara de Diputados, encargada de su revisión.

Esta iniciativa contempla en primer lugar "la integridad física y psíquica de las personas, a través de la protección de la privacidad de los datos neuronales, del derecho a la autonomía o libertad de decisión individual, y del acceso sin discriminaciones arbitrarias a aquellas neurotecnologías que conlleven aumento de las capacidades psíquicas"; garantiza la información a los usuarios de neurotecnologías; define los conceptos de datos neurológicos y neurotecnologías; establece que los datos neuronales constituirán una categoría especial de derechos sensibles de salud de conformidad con la ley 19.628; promueve la investigación científica, pero limitándola al consentimiento informado y libre albedrío de las personas involucradas y homologa la recopilación, almacenamiento, tratamiento y difusión de los datos neuronales y la actividad neuronal de las personas al trasplante y donación de órganos, incluyéndolos en el Código Sanitario y haciendo aplicables las disposiciones que regulan esta materia para estos efectos (Comisión de Desafíos del Futuro, Ciencia, Tecnología e Innovación, 2020).

3) Inteligencia Artificial:

Otro caso en que la explotación de bases de datos masivas, que no necesaria o únicamente se componen de datos personales y/o sensibles, ha comenzado a generar escenarios conflictivos se da en el creciente y cada vez más rápido avance de la inteligencia artificial.

Veíamos al comienzo de este trabajo el impacto que pueden tener los sistemas de segmentación y direccionamiento de la información con fines políticos sobre las sociedades y los sistemas democráticos liberales. La incorporación desregulada de herramientas de aprendizaje y complejización de los sistemas de perfilamiento de los ciudadanos pueden agudizar la segregación de las sociedades en burbujas de reverberancia de determinadas matrices de pensamiento y opinión que, en muchos casos, no se condigan con la realidad y, dado su creciente aislamiento, se vean cada vez más exentas de la necesidad de dialogar con los hechos comprobables y la ciencia, como hemos visto más recientemente en la vehemencia de los movimientos terraplanistas y antivacunas en plena pandemia o aquellos que, sin aportar evidencia significativa, han negado la validez de resultados electorales en diversos países, como Bolivia, Perú, Estados Unidos y, más recientemente Brasil, con las importantes fracturas que estas aseveraciones imprimen en las poblaciones de estos países.

Sin perjuicio de lo anterior, este breve punto expondrá puntualmente el caso de Sophia, la robot humanoide provista de Inteligencia Artificial y diseñada para actuar y aprender como una persona, vale decir, para entablar conversaciones, gesticular y desenvolverse asertivamente frente a su interlocutor, así como para asumir una amplia diversidad de tareas que cada vez logra desempeñar con mayor precisión gracias a su rápido acceso a grandes bases de datos y a la capacidad de procesarlos a gran velocidad generando patrones de comportamiento sobre la información que recibe. Desde su activación en 2015, ha tenido numerosas apariciones públicas, se ha entrevistado con diversas celebridades, fue presentada a las Naciones Unidas y se convirtió en el primer robot en adquirir ciudadanía en un país, la que le fue otorgada el 25 de octubre de 2017 por Arabia Saudita en el marco de su apuesta por diversificar la economía del país poniendo énfasis en la robótica y la tecnología (Buller, 2017) (BBC Mundo Tecnología, 2017). No obstante, el otorgamiento de ciudadanía a un robot, sin perjuicio de tener una finalidad preponderantemente simbólica, constituye un hito controversial que ha gatillado numerosas críticas e interrogantes respecto de las implicancias derivadas de esta nueva calidad, a saber, las dudas acerca de si acciones como su desconexión, omisión de recarga de baterías o borrado de memoria podrían llegar a ser sancionadas como formas de homicidio; ¿Puede ejercer legítima defensa?, la discusión acerca de si, en tanto ciudadana, Sophia adquiere también el derecho a votar en los comicios del país y bajo qué influencias, así como si puede tener un estado civil y cuáles le serían aplicables. No conforme con lo anterior, esto ocurre en un país en que hombres y mujeres no comparten un mismo estatus social, existiendo numerosas restricciones impuestas a la población femenina por motivos religiosos que les significan obligaciones y prohibiciones adicionales, como la imposición de una forma de vestimenta que les impide mostrar la mayor parte de su cuerpo, la obligación de ser acompañadas por un hombre en espacios públicos, la necesidad de un permiso de un familiar masculino para poder trabajar y, hasta hace poco, la prohibición de manejar, entre muchas otras que, no obstante, no se aplicarían a Sophia a pesar de haber sido reconocida como una ciudadana de sexo femenino, lo que de inmediato despertó inquietud por cuanto la robot gozaría en este momento de más derechos que el resto de sus conciudadanas saudíes.

Sophia fue todavía más allá durante 2021, año en que pintó y subastó su primera obra de arte –naturalmente despertando la duda acerca de si aquello podía ser considerado arte y, junto con ello, poniendo en un plano concreto la discusión acerca de si son adjudicables derechos de autor sobre esta obra-, tuvo una modesta participación atendiendo a los periodistas en la entrega de datos sobre participación y resultados en la jornada de elección de la Asamblea de la Comunidad de Madrid y fue anunciada su producción en masa con el objetivo de cumplir funciones de acompañamiento en el contexto de la pandemia de Covid-19 (Vargas, 2021) (García, 2021) (Sánchez, 2021).

Con todo, la mayor parte de las interrogantes asociadas a los avances que se pueden visualizar en el desplante de esta robot se encuentran en un plano primordialmente especulativo, pero el hecho de que en un país ya se encuentre constituida la realidad jurídica de haberse otorgado ciudadanía a un robot, sin distinguir un estatuto especial al efecto, da lugar a todas estas cuestiones y más que son necesarias de abordar para perfilar la manera óptima, tanto social como jurídica, de establecer una adecuada convivencia con robots el día de mañana, cuando, con sus con todas sus particularidades, integren los espacios hasta hoy humanos de una manera más cotidiana.

En este sentido, el reciente lanzamiento en octubre de 2021 de una Política Nacional de Inteligencia Artificial, impulsada por el Ministerio de Ciencia y Tecnología y con una importante participación ciudadana, grupos de interés y de expertos, ha intentado perfilar una hoja de ruta para la utilización, masificación, provecho y desarrollo de la inteligencia artificial en el país por medio del establecimiento de 70 acciones prioritarias a cumplir en 10 años y el establecimiento de tres ejes fundamentales, a saber: (Ministerio De Ciencia, Tecnología, Conocimiento E Innovación, 2021)

- Los factores habilitantes: Elementos que permiten el desarrollo de la inteligencia artificial en el país, como el desarrollo de talentos e infraestructura.
- Desarrollo y adopción: Determina la esfera de desarrollo, es decir, los creadores, proveedores, la demanda de servicios, la transferencia tecnológica, el rol del Estado, los privados y la sociedad civil, la academia, el emprendimiento y sus ámbitos de aplicación.
- Ética, aspectos normativos, y efectos sociales y económicos: Este eje apunto a identificar los potenciales conflictos que puede suscitar la utilización de este tipo de tecnologías y anticiparse a sus respuestas, así como a la referencia y perfilamiento del entramado ético y normativo aplicable al efecto.

La importancia de esta iniciativa es que abre la posibilidad de iniciar, bajo directrices razonables, la investigación y desarrollo masivo de este tipo de tecnologías, así como de sus aplicaciones médicas, previniendo los usos potencialmente abusivos y lesivos de la información sensible de las personas involucradas desde mucho antes que estas sean sometidas a los estudios en cuestión, situación que contrasta radicalmente con la lenta y siempre tardía implementación de las normas de protección de datos personales que, como hemos podido ver, llevan décadas de retraso respecto de los avances tecnológicos a los que apuntan y de los usos masivos de las bases de datos que involucran.

4) Blockchain:

Otro fenómeno de enorme envergadura, aunque de momento parezca un poco más lejano, corresponde a los sistemas de procesamiento de información organizada como cadenas de bloques, esto es el arribo del Blockchain y sus múltiples implicancias potenciales sobre los sistemas jurídicos.

Este mecanismo de registro de información nacido el año 2009 con el objeto de comercializar Bitcoins consiste, a grandes rasgos, en una estructura que ordena unidades de información en bloques dispuestos en una cadena que da cuenta de su cronología. Los bloques creados en Blockchain no pueden ser eliminados ni modificados, pero pueden crearse bloques adicionales que señalen las correcciones pertinentes al bloque original, de manera que no cabe duda acerca de la ocurrencia de los actos que se han puesto en línea y la trazabilidad de los datos se vuelve mucho más segura y certera.

La red creada de este modo se caracteriza por ser absolutamente descentralizada, vale decir, no cuenta con un servidor principal que almacene los datos y depende por completo de las interacciones de todos sus usuarios por igual. Estos usuarios, que funcionan como nodos dentro del esquema, pueden subir los bloques de información que estimen conveniente en forma encriptada y pueden decidir quiénes están facultados para acceder a tales contenidos, siendo segura la comunicación para los involucrados (Barranco, 2019).

Aunque se discute si esto supone una ventaja o desventaja, al tratarse de una red completamente descentralizada, no existe una entidad a la que recurrir o frente a la cual quejarse en caso de olvidar las claves, encontrar contenido difamatorio o perjudicial para una persona o hacer frente a prácticas ilegales en línea, como tampoco es posible ejercer un rol de control sobre las operaciones, por ejemplo financieras, por parte de bancos, superintendencias u otros organismos de fiscalización, lo que garantiza amplias libertades para los usuarios y una especie de necesidad de autorregulación de los mismos respecto de sus actuaciones en la red. Es en vista de ello, y de su calidad de relación económica entre privados, que las operaciones y transacciones ocurridas en su interior deben ser consideradas y posibles de abordar también por el derecho, pudiendo ser necesarias nuevas formas de aportación de pruebas y mecanismos para incorporar las diversas implicancias de este fenómeno a nuestra cotidianeidad jurídica.

Pero el potencial de aplicaciones del Blockchain no acaba en las particularidades de las relaciones entre individuos, sino que ya en la actualidad tiene una enorme variedad de usos, siendo muchas las alternativas que ofrece a futuro y que podrían implicar la masificación de estas plataformas.

Como destaca Brigit Clark, sólo en materia de propiedad industrial, el Blockchain podría utilizarse para probar la "paternidad y autenticación de origen, registro y gestión de los derechos de PI; control y seguimiento de la distribución de los derechos de PI, registrados o no; prueba de uso efectivo o primer uso comercial; gestión electrónica de los derechos (por ejemplo, sitios de música en línea); establecimiento y observancia de acuerdos de PI, licencias o redes de distribución exclusiva mediante

contratos inteligentes; y transmisión de pagos en tiempo real a los titulares de derechos de PI. La cadena de bloques también se puede utilizar con fines de autenticación y determinación del origen en los procesos de detección o recuperación de mercancías falsificadas, robadas y de importación paralela" (Clark, 2018).

Atendiendo a su carácter descentralizado, sistema de cifrado, accesos controlados por el dueño de la información y la inmutabilidad de la información, que vuelve innecesarios los ministros de fe para dar cuenta de actos jurídicos de connotación pública, durante los últimos años se ha propuesto avanzar en reemplazar los burocráticos y caros Conservadores de bienes raíces por sistemas en Blockchain para el registro de propiedad de la tierra (Hermann, 2018), para lo que ya se han dado los primeros pasos reuniendo al equipo de Gobierno Digital con representantes de los Conservadores de bienes raíces y Tesorería General de la República en orden a implementar un primer plan piloto de esta modalidad (Editor Revista Fojas, 2018).

Si puede hacerse una modificación de tal magnitud con los Conservadores de bienes raíces, puede ocurrir lo propio con los Registros de Comercio, y Notarías, todas estas instituciones altamente concentradas, lentas y costosas en términos de operatividad que, pese a la desactualización y extrema burocracia de sus mecanismos de registros, se hallan anquilosadas en nuestro sistema sin haber sido adaptadas significativamente para hacer frente a los niveles de información acumulados, a las dimensiones del público y los trámites que deben atender a diario.

Modificar estas oficinas de registros por sistemas de organización de sus datos en Blockchain podría simplificar y abaratar una multiplicidad de trámites, desde los requisitos y formas de transferencia de la propiedad, prueba de los pagos, verificación de la vigencia de títulos, propiedades y sociedades, inscripción de modificaciones y un largo etcétera que supondrían un verdadero terremoto procesal para los procedimientos e instituciones a los que nos encontramos acostumbrados.

Sin perjuicio de lo anterior, no deja de ser cierto que Blockchain, en sí, no es más que un sistema de registro ordenado y de alta fidelidad, pero incapaz de discriminar las operaciones que ocurren en su interior, de manera que no puede corroborar los requisitos de existencia y validez de los actos jurídicos, como pueden ser la capacidad de las partes para actuar, la comprobación de la titularidad sobre un derecho determinado, la libertad del consentimiento, entre otros; de modo que, si bien puede facilitar, abaratar y dinamizar estos trámites en forma contundente, no parece sustituir del todo la función de controlar la legalidad de los actos que corresponde actualmente a los jefes de servicio de estas instituciones.

Con todo, es fundamental comenzar a observar el funcionamiento de esta forma de procesamiento de bases de datos masivas que más pronto que tarde se encontrará en condiciones de revolucionar

nuestros modelos registrales con todas las implicancias que ello acarree para los actuales sistemas jurídicos.

5) Nueva Constitución y decisiones judiciales automatizadas:

Este ha sido uno de los temas centrales abordados por el presente trabajo en relación con los desafíos y marcos de posibilidad que se vislumbran para la aplicación del Big Data en ámbitos de relevancia jurídica. Hasta aquí hemos visto los marcos normativos aplicables en la Unión Europea, en el Chile actual y el que se halla próximo y, con bastante interés, la regulación estonia, cuyo contexto podría permitirnos analizar los resultados empíricos de las primeras judicaturas robot del mundo, junto con los requisitos especiales para su funcionamiento.

En cualquier caso, lo que ya es una realidad es el apoyo provisto por diversos programas dotados de inteligencia artificial en el campo de la adjudicación de justicia, lo que supone una esfera de propuesta o de toma de decisiones automatizadas que pueden afectar significativamente a las personas. Si bien el uso de estos sistemas suele ser secundario y cumple un rol auxiliar para usar como base o antecedente en resoluciones oficiales, su sola utilización constituye razón suficiente para la toma de medidas adicionales de resguardo de los derechos y libertades de las personas afectadas y, por supuesto, una mayor exigencia e implementación de protocolos adicionales para las instituciones involucradas, todo lo cual pudimos revisar con mayor detalle en los capítulos anteriores.

Sin perjuicio de ello, y aun teniendo en cuenta el ámbito de aplicación que las normas analizadas permiten para este tipo de tecnologías, su creciente utilización y la diversificación de sus funciones e influencia suponen un desafío considerable para lograr armonizar en los próximos años los enormes aportes que pueden llegar a realizar estas herramientas con el adecuado resguardo de las garantías fundamentales.

Ahora, más allá de los referidos cambios legislativos que avanzan en Chile, existe otro hito de gran relevancia para el país, a saber, el resultado de la propuesta constitucional que emane de la Convención Constitucional y el subsecuente resultado del plebiscito que podría validar o rechazar el texto con todas las implicancias políticas, sociales y legales que de ello podrían derivar.

En lo que concierne a la factibilidad futura de tomar decisiones judiciales automatizadas, es necesario observar nuevamente los principios y objetivos que podría cimentar una nueva carta fundamental. En este sentido, la eventual aprobación de una nueva Constitución difícilmente incidiría de manera significativa en el contenido de los proyectos de ley revisados cuya promulgación se encuentra

próxima, sin perjuicio de lo cual puede llegar a delimitar de manera distinta los derechos y garantías de las personas a las que tanto hemos hecho referencia en este trabajo, de manera que podría cambiar el objeto último de protección de las nuevas normas, aspecto de suma relevancia a la hora de ponderar los efectos prácticos de la implementación y regulación del Big Data en los sistemas judiciales. Asimismo, puede haber modificaciones en las definiciones y misiones del Estado que pueden resultar significativos, ya sea acelerando o ralentizando los procesos de transición tecnológica de sus instituciones.

Considerando lo anterior, cerraremos este trabajo con la revisión de algunos puntos del consolidado de normas aprobadas por la Convención Constitucional[14] que podrían llegar a incidir en esta materia (Convención Constitucional, 2022).

Lo primero a destacar es que en la sección encargada de describir los sistemas de conocimiento se aprobó el derecho a la protección de los datos personales bajo el enunciado "Todas las personas tienen derecho a la protección de los datos de carácter personal, a conocer, decidir y controlar el uso de las informaciones que les conciernen". Lo interesante de este punto es que con esta redacción se supera el marco de protección anterior al constitucionalizarse la protección no sólo de los datos personales, como contempla la Constitución actual en su artículo 19 n°4, sino también de los derechos de acceso e información sobre los datos tratados y sus usos y el derecho a oponerse al tratamiento en cuestión. Lo que se deberá determinar a este respecto es si el derecho a decidir los usos tendrá una aplicación *ex ante* o *ex post*, para lo cual deberán utilizarse los parámetros anteriormente revisados para la aplicación de los derechos ARCOP. Naturalmente, es posible que este punto sea objeto de controversia si algunas partes estiman que la forma de resguardo legal de este derecho resulta muy restrictiva atendido su nuevo rango constitucional.

En la misma sección, la Convención aprobó el derecho a la seguridad informática señalando que "Todas las personas, individual y colectivamente, tienen el derecho a la protección y promoción de la seguridad informática. El Estado y los particulares deberán adoptar las medidas idóneas y necesarias que garanticen la integridad, confidencialidad, disponibilidad y resiliencia de la información que contengan los sistemas informáticos que administren, salvo los casos expresamente señalados por la ley". Así, se constitucionaliza igualmente la seguridad informática, pero los parámetros y mecanismos para hacer efectivo este derecho quedarán encargados a leyes y reglamentos, por lo que la incorporación de esta norma no debiera cambiar lo que ya hemos revisado sobre este tema.

Sin perjuicio de encontrarse avanzado el proyecto de ley que crea una Agencia Nacional de Protección de Datos Personales, la Convención ha decidido dar rango constitucional a este organismo al

[14] Al momento de escribir estas líneas, el consolidado corresponde al primer borrador de texto, que será entregado a las comisiones de armonización y de normas transitorias para terminar de pulir la propuesta que será plebiscitada.

contemplar su creación igualmente en la propuesta, donde se consagraría su carácter autónomo y su misión de investigar, normar, fiscalizar y sancionar la promoción y protección de los datos personales tratados por entidades públicas y privadas, quedando encargada a la ley la determinación de sus atribuciones, composición y funciones.

Respecto del principio de transparencia que rige al Estado en la actualidad, la propuesta de la Convención mantiene la línea actual estableciendo que es pública la información elaborada con presupuesto público y toda aquella que obre en poder del Estado, salvo cuando su publicidad afectare el debido cumplimiento de los órganos del Estado, la protección de los datos personales, los derechos de las personas, la seguridad del Estado o el interés nacional, por lo que se mantiene la limitante de afectación a la privacidad a la hora de determinar la entrega o no de datos en manos del Estado.

En adición, se pone énfasis a la innovación y modernización del Estado, el que deberá utilizar "los mejores avances de las ciencias, tecnología, conocimientos e innovación para promover la mejora continua de los servicios públicos". Asimismo, se establece que "Es deber del Estado definir mecanismos de modernización de sus procesos y organización, ajustando su funcionamiento a las condiciones sociales, ambientales y culturales de cada localidad. [] El Estado deberá destinar recursos para que sus órganos adopten las medidas que resulten necesarias para la incorporación de avances tecnológicos, innovación y el mejor uso de los recursos que permitan optimizar la provisión de bienes y servicios públicos".

Estos últimos dos artículos dan cuenta de la necesaria tecnologización e innovación que requerirá el Estado, que deberá adoptar sostenidamente nuevos mecanismos de gestión para adaptarse y, como dicen las normas citadas, utilizar las ciencias y tecnologías para ajustar su funcionamiento mejorando los servicios públicos. Tales máximas, por supuesto, no son una invitación directa a la implementación de sistemas de inteligencia artificial o de adopción de programas de decisiones automatizadas en sede judicial, no obstante, presentan un enfoque para la administración pública que tiene en cuenta la necesidad de brindar a la ciudadanía una administración eficiente de los servicios públicos, para lo cual será primordial tener en consideración los paradigmas de época en ciencia y tecnología. Ello implica, cuando menos, considerar los sistemas de toma de decisiones automatizados en diversos ámbitos e instituciones, debiendo ponderar su potencial tanto de mejorar la velocidad y calidad del servicio, como de lesionar los derechos y libertades de las personas y la capacidad técnica y económica de adoptar medidas de seguridad que disminuyan sus riesgos asociados.

Teniendo esto en consideración, no parece que el texto propuesto por la Convención restrinja la posibilidad de incorporar mecanismos de toma de decisiones automatizadas en sede judicial más allá de lo que lo hace el propio proyecto de ley sobre protección de datos personales. Por el contrario, la

prerrogativa que se da al Estado de modernizarse, innovar y aprovechar al máximo los avances en diversas áreas del conocimiento, abre la puerta a que en un futuro cercano puedan adoptarse estas tecnologías, lo que podría permitirnos una tramitación judicial más expedita y capaz de procesar una cantidad mucho mayor de información.

De tal manera, y habiendo llegado a la conclusión de que nuestro próximo esquema normativo admitirá la incorporación de programas automatizados que coadyuven a la toma de decisiones judiciales cumpliendo un rol auxiliar, y siempre quedando encargada la resolución final a un ser humano debidamente capacitado tanto en el derecho como en la forma de funcionamiento de dicho programa, el desafío que plantea este punto tiene que ver, por un lado, con el perfeccionamiento de los sistemas a utilizar, con su adecuado entrenamiento que sea capaz de evitar sesgos, con la capacidad de comprender el razonamiento que aplica el programa para resolver evitando así espacios de opacidad, con el entrenamiento y capacitación humana que se requerirá al interior del Poder Judicial, desde el personal administrativo hasta los jueces, para poder emplear estos programas de un modo que resguarde los derechos de los involucrados, con el establecimiento de mecanismos de información adecuados para la ciudadanía y de procedimientos pertinentes que faciliten el ejercicio de sus derechos y con el despliegue de sistemas de seguridad informática acordes a la envergadura tanto de la función pública como de la sensible información que tratarían los tribunales.

CONCLUSIONES

Hay una serie de ideas que se desprenden tras revisar estos capítulos. La primera de ellas es que cuando hablamos de tecnología, debemos entender que esta posee un carácter esencialmente neutro y que cada nuevo método tiene un enorme potencial de usos que pueden sumar o restar a las comunidades.

Es interesante analizar cómo, a un mismo tiempo, la inteligencia artificial puede usarse para salvar vidas y para manipular las democracias. Una ambivalencia de la que tenemos que ser conscientes y responsabilizarnos como sociedad.

De un tiempo a esta parte, los datos se han convertido en un activo sumamente valioso y cotizado en abundancia, no obstante, su concentración otorga al tenedor un gran poder y una condición de asimetría respecto del titular de la información o de aquel a quien puede llegar a afectar. De manera que la facultad de utilizarla y, más aun, el incentivo al desarrollo de mecanismos cada vez más avanzados que permitan realizar nuevas tareas en forma veloz y precisa debe ir acompañado de un sistema de normas que tiendan a equilibrar la situación y que conviertan la innovación en un aporte capaz de emplearse para beneficio de las mayorías y, junto con ello, de instituciones capaces de hacerlas cumplir. O cuando menos debe existir la preocupación por que estas últimas no queden muy atrás en una carrera que, naturalmente, han comenzado rezagadas.

Siguiendo con lo anterior, otro punto que no puede dejar de recogerse es la evidente diferencia en los plazos de evolución de la tecnología y la ley, toda vez que la última tiende a responder al fenómeno una vez que este existe y ya ha causado efectos dignos de atención. Es por ello que al momento de pensar y aplicar reglas que regulen campos científicos y tecnológicos es necesario hacer el esfuerzo de abstraer los casos concretos a líneas generales de comportamiento y a la reflexión acerca del objetivo que pretendía la norma. Con esto y la flexibilización interpretativa de su contenido será posible subsumir hipótesis que no necesariamente hubieran sido previstas al momento de su creación, pero que resultan atingentes con miras al objeto perseguido por el legislador. Lo anterior, no obstante, ha de restringirse para casos de aplicación de normas penales bajo el principio de *nullum crimen, nulla poena sine lege praevia e stricta*. Con todo, la ampliación de criterios de aplicación en los términos referidos facilitaría enormemente la toma de mayores resguardos por parte del regulado y el ejercicio de la ley para el fiscalizador.

Otro factor que esta investigación permite destacar es que, sin perjuicio de los puntos anteriores, en sólo 30 años hubo un enorme salto en la concientización de los resultados omnímodos derivados de la democratización de las tecnologías de la información y de la centralización de los servidores y los datos que esta genera. La evolución y sofisticación de las leyes creadas al efecto dan cuenta de ello pese a sus vacíos. Pero más importante que estas leyes individualmente consideradas, es la conclusión a la que paulatinamente ha llegado la comunidad internacional respecto de la necesidad de homologar en la mayor medida posible los marcos normativos que rigen las actividades de tratamiento de información, puesto que, en un mundo interconectado a este punto, se convierte en una realidad prístina el hecho de que los fenómenos asociados, a saber, la prestación de servicios, las faltas, vulneraciones y delitos que involucran el tratamiento de datos ocurren simultáneamente y de manera interdependiente en distintos lugares del globo, por lo que su respuesta debe provenir asimismo de todos estos lugares y del modo más coherente y sistemático posible. Hacer frente a un problema cuya cadena de procesos se extiende más allá de las fronteras requiere de un alto poder de coordinación y colaboración por parte de los países involucrados y esta es una de las principales razones por las que vale la pena celebrar las medidas de resguardo sobre la información que los países de la Unión Europea exigen al momento de firmar tratados o acuerdos comerciales, así como también la lógica de cooperación que demanda el Convenio de Budapest de sus miembros y la Red 24/7, cuya función trasciende a los delitos informáticos y establece una vía de apoyo mutuo entre las instituciones encargadas de la investigación de delitos en cada país cuando a propósito de la comisión del ilícito perseguido se hubiera utilizado alguna tecnología de la información foránea.

Entre los grandes aportes del RGPD y las normas más modernas sobre el tratamiento de datos personales, hay que poner de relieve el nuevo derecho a la impugnación de decisiones automatizadas en tanto medida que tiene a la vista, por un lado, las limitaciones de los programas de procesamiento de información, y por otro, la primitiva capacidad de análisis que logran ostentar nuestras mejores inteligencias artificiales cuando se trata de decisiones con repercusiones directas sobre las personas. Aunque no sabemos el grado de complejidad con que las máquinas podrán resolver este tipo de asuntos en el futuro, lo cierto es que hoy resulta absolutamente necesario velar por la participación de seres humanos en la toma de decisiones que afectan a otros humanos. Ello, claro, no obsta la posibilidad de considerar la propuesta de una máquina, o de someter ciertos asuntos a su revisión, pero tras leer estas líneas sabemos que, por lo pronto, la aplicación de criterio humano para la toma de decisiones que conciernen a otros constituye una garantía que no se puede soslayar.

Así, uno de los grandes retos que enfrentará Chile en los próximos años, una vez que las nuevas leyes de protección de datos personales y de delitos informáticos entren en vigencia, será desarrollar un

entramado institucional robusto, capaz de hacerlas efectivas y de, finalmente, dar la relevancia que corresponde a la privacidad y a las esferas de reverberancia de la información a fin de evitar que este nuevo entramado de normas se convierta en letra muerta como ocurrió con la ley 19.628.

Dentro de este mismo reto se encuentra la formación de un criterio flexible de análisis que permita aplicar razonablemente las premisas a los hechos manteniendo el respeto por los principios y objetivos de la ley siempre que se enfrente a nuevas hipótesis y tecnologías.

En este sentido, un caso emblemático para nuestra disciplina es la incorporación de programas de toma de decisiones automatizadas en sede judicial y, junto con ello, la posibilidad de establecer jueces robot que eventualmente puedan resolver causas sometidas a su conocimiento.

Tras una vasta revisión de estas posibilidades en el escenario actual, parece bastante claro que, hasta aquí, no existirían condiciones propicias para pensar en que se pueda asignar a una inteligencia artificial la delicada tarea de fallar controversias que involucran fuertes componentes de relacionamiento humano. Si bien existen ya contratos inteligentes capaces de contemplar distintas alternativas al momento de su celebración y de ejecutarse automáticamente de acuerdo a la verificación de una de ellas cumpliendo con la condición pactada, es claro que ejercicio de una judicatura resulta un ejercicio mucho más complejo y variable que tendrá que esperar.

Sin embargo, la situación de los programas de toma de decisiones automatizadas capaces de apoyar la tarea jurisdiccional supone un caso diferente, pues habida cuenta de la enorme cantidad de información con que deben lidiar jueces y funcionarios para cumplir su labor, así como también la extensa burocracia que caracteriza al sistema judicial, parece incluso conveniente avanzar en su integración, acotando su operación a objetos específicos, como una revisión expedita de jurisprudencia, el relleno automático de documentos tipo, la organización de turnos y agendas, la preparación y envío de oficios, etc.

Pero, existiendo la habilitación legal, su función no tiene por qué limitarse al mero apoyo administrativo, sino que también puede aportar en materias de fondo, como en la resolución de materias de tránsito que requieran del análisis de fotografías u otros documentos, en la ponderación predictiva de comportamiento para efectos de determinar medidas cautelares, beneficios carcelarios o suspensiones condicionales del procedimiento o en la propuesta de sentencias, como vimos que ocurría con el *software* Prometea. Todo esto, por supuesto, bajo supervisión humana competente, es decir, capacitada tanto en la ley como en el método aplicado, que revise los resultados y esté en condiciones de controvertirlos en caso de ser aplicable algún elemento de análisis adicional que pueda haber sido omitido o sopesado malamente por las máquinas, y, en su defecto, garantizando una instancia de impugnación que otorgue a los afectados la posibilidad de disputar un resultado gravoso emitido por un algoritmo y que no hubiera

sido revisado por un ser humano o cuya revisión hubiere sido una mera formalidad o de carácter deficiente.

Asimismo, y tratándose de asuntos tan sensibles para los involucrados, es necesario el establecimiento de elevados protocolos y de esquemas de cumplimiento estrictos que contemplen la permanente actualización y perfeccionamiento de los programas, un entrenamiento de *software* acorde a los estándares a aplicar, que evite sesgos, filtraciones o usos perjudiciales e inapropiados de la información, que propendan a disminuir los márgenes de opacidad y que tengan siempre a la vista que es fundamental la adecuada capacitación de jueces y funcionarios para un uso virtuoso de los sistemas.

De tal manera, se estima que la implementación de estos mecanismos puede acarrear importantes mejoras a la administración de justicia, generando una mayor homologación de criterio, aumentando la velocidad y capacidad de análisis por caso, disminuyendo la carga laboral a los funcionarios, acelerando la tramitación de la comunicación entre instituciones, incrementando la velocidad en la redacción de sentencias, generando propuestas más precisas en relación con los datos analizados y un largo etcétera que podrían tener como resultado un sistema judicial menos burocrático, más expedito y confiable.

Este punto resulta sumamente interesante también porque si algo podemos destacar de este momento en la historia del derecho, es que hoy se encuentra sometido a un nivel de estrés bastante inédito en cuanto a sus procedimientos, toda vez que, en un contexto de gran saturación administrativa, por primera vez en siglos se presenta la posibilidad y el deber de innovar radicalmente respecto de los métodos que siempre se han empleado para enfrentar las controversias jurídicas. Estamos en un punto en que esta disciplina, que siempre se ha jactado de sus formas y su tradición, se está viendo superada por una realidad sumamente veloz que ocurre en un mundo interconectado y en el que todo es información. De ahí que los debates sobre incorporar programas provistos de inteligencia artificial y capaces de resolver asuntos de manera automatizada adopten una enorme envergadura, pues se trata de una alteración en muchos de los cimientos del sistema, una afectación (no necesariamente peyorativa) al debido proceso, a la forma de lograr mayores niveles de igualdad ante la ley, el hecho de incorporar formas de raciocinio no enteramente humanos, a veces ininteligible, y mucho más, lo que supone un extraordinario desafío, tanto para la teoría como para la *praxis* que, a estas alturas, parece ineludible.

Bibliografía

Acta de Protección de Datos Personales. Estonia.

Adquisición decontrol sobre Delivery Technologies SpA por parte de Walmart Chile, FNE161-2018 (Fiscalía Nacional Económica 11 de Enero de 2019). Recuperado el 2 de Abril de 2021, de https://www.fne.gob.cl/wp-content/uploads/2019/01/Informe-de-aprobaci%C3%B3n-F-161-2018-censurado.pdf

Agencia Española de Poritección de Datos . (2015). *Memoria Agencia Española de Protección de Datos 2014.* Madrid.

Agencia Española de Protección de Datos. (2016). Orientaciones y garantías en los procedimientos de ANONIMIZACIÓN de datos personales. Madrid, España.

América Economía. (19 de 10 de 2018). Tribunal Electoral de Brasil busca contener difusión de "fake news". Brasil.

Ariel Podestá, S. L. (2019). Beneficios del uso de Big Data en la Justicia. Análisis de su aplicación sobre el software INVESTIGA. *Research Gate*.

Article 29 Working Party (WP29). (2014). *Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU.* Bruselas.

Ávalos, F. A. (2014). Las fuentes de acceso público a datos personales. *Revista Chilena de Derecho y Tecnología*, 205-226.

Bachelet, M. (2017). *Mensaje 001-365.* Santiago.

Barranco, M. (14 de 03 de 2019). *Finanzas Digitales: revolución en el ámbito financiero.* Recuperado el 15 de 10 de 2021, de https://www.youtube.com/watch?v=mq1oMzuwqqg

Bauzá, V. H. (2017). Tecnologías para la Privacidad y la Libertad de Expresión: Reglas sobre Anonimato y Cifrado. Santiago, Chile.

BBC. (20 de Octubre de 2018). Elecciones en Brasil: por qué WhatsApp bloqueó la cuenta del hijo de Bolsonaro y la de cientos de miles de usuarios en las vísperas de los comicios. Washington D.C., EE.UU.

BBC Mundo Tecnología. (30 de 10 de 2017). Sophia, la robot que tiene más derechos que las mujeres en Arabia Saudita. Recuperado el 31 de 07 de 2021, de https://www.bbc.com/mundo/noticias-41803576

Buller, A. (25 de 10 de 2017). Saudi Arabia announces $500 billion city of robots and renewables. Arabia Saudita. Recuperado el 03 de 08 de 2021, de https://www.arabnews.com/node/1182501/saudi-arabia

Bundeskartellamt. (2019). *Bundeskartellamt prohibits Facebook from combining user data from different sources.* Bonn, Alemania. Recuperado el 09 de agosto de 2020, de https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook_FAQs.pdf?__blob=publicationFile&v=5

Cerdeira, L. (20 de Septiembre de 2020). Lo que podemos aprender de Estonia, el país más digitalizado del mundo. *Forbes*. Obtenido de https://forbes.es/empresas/76138/lo-que-podemos-aprender-de-estonia-el-pais-mas-digitalizado-del-mundo/

Cerna, T. (14 de mayo de 2020). *emol*. Recuperado el 14 de mayo de 2020, de https://www.emol.com/noticias/Nacional/2020/05/14/986040/Ciberdelitos-pandemia-pdi.html

Chief Science Office, Gemeente Amsterdam. (20 de Abril de 2022). *City of Amsterdam Algorithm Register Beta*. Obtenido de https://algoritmeregister.amsterdam.nl/en/ai-register/

Clark, B. (Febrero de 2018). La tecnología de la cadena de bloques y el Derecho de propiedad intelectual: ¿una pareja perfecta en el criptoespacio? Londres, Inglaterra. Recuperado el 16 de Octubre de 2021, de https://www.wipo.int/wipo_magazine/es/2018/01/article_0005.html

CNN. (23 de 10 de 2018). Moon Ribas: La bailarina cyborg que puede detectar terremotos. Recuperado el 16 de 06 de 2021, de https://edition.cnn.com/videos/spanish/2018/10/23/luna-ribas-cyborg-inteligente-creatividad-baile-digital-original.cnn

Comisión de Desafíos del Futuro, Ciencia, Tecnología e Innovación. (2020). *Proyecto de Ley:Sobre protección de los neuroderechos y la integridad mental, y el desarrollo de la investigación y las neurotecnologías.* Valparaíso.

Comisión Desafíos del Futuro, Ciencia, Tecnología e Innovación. (2019). *Hacia una estrategia nacional de Inteligencia Artificial.* Santiago.

Comisión Europea. (2020). *Propuesta de Reglamento sobre mercados disputables y equitativos en el sector digital (Ley de Mercados Digitales).* Comisión Europea. Recuperado el 2 de Abril de 2021, de https://eur-lex.europa.eu/legal-content/es/TXT/?qid=1608116887159&uri=COM%3A2020%3A842%3AFIN

(s.f.). *COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL.*

Convención Constitucional. (2022). *CONSOLIDADO NORMAS APROBADAS PARA LA PROPUESTA.* Santiago.

Dance, M. R. (10 de Abril de 2018). Así funcionaba la recolección de datos de Cambridge Analytica. *New York Times*.

Daniel Martin, M. J. (2016). *A General Approach for Predicting the Behavior of the Supreme Court of the United.* Recuperado el 18 de Marzo de 2022, de file:///C:/Users/Fernanda%20Carvajal/Downloads/A_General_Approach_for_Predicting_the_Behavior_of_.pdf

DataIgualdad. (2019). *DataIgualdad*. Obtenido de https://dataigualdad.org/data/questions?country_id=a17116c4-eeda-4b35-be50-989e4ef53196

Dirección General de Redes de Comunicación, Contenido y Tecnologías de la Comisión Europea. (2019). *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Generar confianza en la inteligencia artificial centrada en el ser humano.* Bruselas.

Editor Revista Fojas. (2018). Gobierno Digital: Primera reunión con el CBRS y la TGR para implementar un plan piloto de Blockchain. *Revista Fojas*.

Elsa Esteves, S. L. (2020). *PROMETEA. TRANSFORMANDO LA ADMINISTRACIÓN DE JUSTICIA CON HERRAMIENTAS DE INTELIGENCIA ARTIFICIAL.* Banco Interamericano del Desarrollo, Washington D.C.

Estonia se prepara para tener "jueces robot" basados en inteligencia artificial. (12 de Junio de 2019). Obtenido de The Technolawgist: https://www.thetechnolawgist.com/2019/06/12/estonia-se-prepara-para-tener-jueces-robot-basados-en-inteligencia-artificial/

Evans, D. (2011). *Internet de las cosas: Cómo la próxima evolución de internet lo cambia todo.* Abril.

Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate, B6-22/16 (Bundeskartellamt 15 de Febrero de 2019). Recuperado el 1 de Abril de 2021, de https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=4

Ferrer, M. T. (2020). *www.ga_p.com.* Recuperado el 2 de Abril de 2021, de https://www.ga-p.com/wp-content/uploads/2020/12/La_Comisio%CC%81n_presenta_DMA.pdf

Gabo, F. (Octubre de 2019). *Youtube*. Obtenido de https://www.youtube.com/watch?v=tco3OSDVXCk

García, J. M. (5 de Mayo de 2021). as limitaciones de Sophia, el robot que participó de la jornada electoral de Madrid. *La Vanguardia*.

Gartner. (2017). *Gartner.* Obtenido de https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

Garvie, C., Bedoya, A., & Frankle, J. (2016). *The Perpetual Line-Up.* Gerogetown Law Center on Privacy & Technology, Gerogetown.

Geoffrey Hinton, Y. L. (2015). Deep Learning. *Review*.

Gobierno de Chile. (2017). *Política Nacional de Ciberseguridad.* Gobierno de Chile. Recuperado el 2020 de junio de 7, de https://www.ciberseguridad.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf

Gold, H. (19 de mayo de 2020). *CNN*. Recuperado el 21 de mayo de 2020, de https://cnnespanol.cnn.com/2020/05/19/hackeo-a-easyjet-roba-datos-de-9-millones-de-clientes-y-miles-de-numeros-de-tarjetas-de-credito/

González, K. (15 de Mayo de 2019). ¿Qué son las ciudades inteligentes? Santiago está en el top 1 de Latinoamérica según ranking internacional. *La Tercera*.

Grupo de Trabajo sobre Protección de Datos del Artículo 29. (2018). *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679.* Bruselas. Recuperado el 7 de Septiembre de 2020, de https://www.aepd.es/sites/default/files/2019-12/wp251rev01-es.pdf

GTD. (2019). *GTD*. Obtenido de https://www.gtd.cl/landings/smart-home?gclid=CjwKCAiAlajvBRB_EiwA4vAqiAHaw9FduvH8nkPOXqg2sUoy-_jSvvf0UPleT-kCJfKm9IRy6spHyxoCMEoQAvD_BwE

Harbisson, N. (3 de Agosto de 2018). El "cyborg" con una antena en su cabeza. *Tele13*. (F. Valenzuela, Entrevistador) Recuperado el 7 de Abril de 2021, de https://www.youtube.com/watch?v=Wr8pIzgmlJY

Hermann, J. (11 de Enero de 2018). Blockchain: El registro de propiedd del futuro. *Diario Financiero*.

IBM. (21 de Marzo de 2022). *¿Qué son los contratos inteligentes en blockchain?* Obtenido de IBM: https://www.ibm.com/cl-es/topics/smart-contracts

Ibrahim Abaker Targio Hashem, V. C. (2016). The Role og Big Data in Smart City. *International Journal of Information Management*.

Julia Angwin, J. L. (23 de Mayo de 2016). *Machine Bias.* Recuperado el 22 de Marzo de 2022, de ProPublica: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

Klare, B., Burge, M., Klontz, J., & Jain, R. V. (2012). Face Recognition Performance Role of Demographic. *IEEE Transactions on Information Forensics and Security*. Recuperado el 19 de junio de 2020, de http://openbiometrics.org/publications/klare2012demographics.pdf

Laborde, A. (8 de Junio de 2019). Un 'hacker' paraliza Baltimore desde hace un mes. *El País*.

Lao, R. (16 de Enero de 2018). *Towards Data Science*. Obtenido de https://towardsdatascience.com/a-beginners-guide-to-the-data-science-pipeline-a4904b2d8ad3

Lara, J. C., Martínez, M., & Viollier, P. (2014). Hacia una regulación de los delitos informáticos basada en la evidencia. *Revista Chilena de Derecho y Tecnología*, 101-137.

Levin, S. (19 de Octubre de 2018). Facebook has a fake news 'war room' - but is it really working? *The Guardian*.

Limón, R. (27 de Marzo de 2019). El 'Nóbel' de la informática reconoce los avances en las redes neuronales. *El País*.

Management Solutions. (2018). *Machine Learning, una piea clave en la transformación de los modelos de negocio.*

Michal Kosinski, D. S. (2013). Private traits and attributtes are predictable from digital records of human behavior. *PNAS*, 5802-5805.

Migliorisi, D. (2014). *Crímenes en la Web, Los delitos del siglo XXI.* Buenos Aires: Editorial del Nuevo Extremo.

Ministerio De Ciencia, Tecnología, Conocimiento E Innovación. (2021). *Política Nacional de Inteligencia Artificial.* Santiago.

Ministerio de Ciencia, Tecnología, Conocimiento e Innovación. (4 de abril de 2022). *Ministerio de Ciencia, Tecnología, Conocimiento e Innovación.* Obtenido de https://minciencia.gob.cl/noticias/chile-presenta-la-primera-politica-nacional-de-inteligencia-artificial/

Onur Varol, E. F. (2017). *Online Human-Bot Interactions:Detection, Estimation, and Characterization*. California, EE.UU.

Perlroth, N., & Shane, S. (25 de Mayo de 2019). In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc. *The New York Times*.

Peter Mell, T. G. (Septiembre de 2011). *NIST*. Obtenido de https://csrc.nist.gov/publications/detail/sp/800-145/final

Philipp Max Hartman, M. Z. (2016). Capturing Value from Big Data - A Taxonomy of Data Driven Business Models Used by Start-up Firms. *International Journal of Operations and Production Management*.

Revista Chilena de Derecho Informático. (Diciembre de 2003). Europa y la Protección de los Datos Personales. *Revista Chilena de Derecho Informático*. Obtenido de Europa y laProtección de Datos Personales: http://web.uchile.cl/vignette/derechoinformatico/CDA/der_informatico_simple/0,1493,SCID%253D14234%2526ISID%253D507%2526PRT%253D14232,00.html

Rosenblut, V. (2008). Punibilidad y tratamiento jurisprudencial de las conductas. *Revista Jurídica del Ministerio Público*, 254-266.

Samsung. (21 de Octubre de 2019). *Samsung*. Obtenido de https://www.samsung.com/cl/refrigerators/french-door-refrigerator-with-family-

hub/?cid=cl_paid_ppc_google-search_family-hub_no-phase_family-hub_local-content_na/cold/competencia/com_serch-none-2019-10-21_all

Sánchez, V. (1 de Febrero de 2021). La robot Sophia será producida en masa para luchar contra el Covid-19. *24 France*.

SERNAC. (1 de junio de 2020). *SERNAC*. Recuperado el 2 de junio de 2020, de https://www.sernac.cl/portal/604/w3-article-58572.html

Siebert, F. (5 de agosto de 2019). Neuroderechos: la discusión por la privacidad mental y el control del cerebro ya está aquí. (U. d. Chile, Ed.) Santiago, Chile. Recuperado el 2 de septiembre de 2021, de https://www.uchile.cl/noticias/156392/neuroderechos-la-discusion-por-la-privacidad-mental

Silva, D. (27 de abril de 2017). Presidenta Bachelet presenta Política Nacional de Ciberseguridad. *La Tercera*.

SOPHOS. (mayo de 2020). *THE STATE OF RAMSOMWARE 2020.* Recuperado el 21 de mayo de 2020, de https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf

Soroush Vosoughi, D. R. (2018). The Spread oftrue and false news online. *Science*.

United States Government Accountability Office (GAO). (2016). *Face Recognition Technology, FBI should better ensure Privacy and Accuracy.* Obtenido de https://www.gao.gov/assets/680/677098.pdf

Universidad de Buenos Aires. (13 de Abril de 2020). *UBAHOY*. Obtenido de https://www.uba.ar/noticia/20195

Vargas, J. G. (7 de Abril de 2021). Una obra de criptoarte creada por una robot se subasta por 580.000 euros. *El País*.

Versión pública de la resolución del expediente CNT-161-2018 , CNT-161-2018 (Comisión Federal de Competencia Económica 5 de Junio de 2019). Recuperado el 2 de Abril de 2021, de https://www.cofece.mx/CFCResoluciones/docs/Concentraciones/V6008/9/4845885.pdf

Victor Mayer-Schönberger, K. C. (2013). *Big Data, La revolución de los datos masivos.* Madrid: Turner.

Viera-Gallo, J. A. (16 de julio de 1991). Moción Parlamentaria en Sesión 19. Legislatura 322. Valparaíso, Chile.

WP 203. (2013). *Opinión 03/2013, limitaciones de la finalidad*. Obtenido de https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

Yuste, R., Goering, S., & otros. (9 de noviembre de 2017). Four ethical priorities for neurotechnologies and AI. Recuperado el 2 de septiembre de 2021, de https://www.nature.com/articles/551159a