DERECHO Y NUEVAS TECNOLOGÍAS

EL IMPACTO DE UNA NUEVA ERA

JHOEL CHIPANA CATALÁN
Coordinador

THĒMIS
EDITORIAL JURÍDICA
JCC | JHOEL CHIPANA CATALÁN

DERECHO
Y NUEVAS
TECNOLOGÍAS
EL IMPACTO DE UNA NUEVA ERA

THĒMIS
desde 1965

Para su sello editorial Editorial Jurídica THĒMIS
Segundo piso de la Facultad de Derecho
Pontificia Universidad Católica del Perú
Av. Universitaria 1801, Lima 32, Perú
Teléfono: 626-2000, anexo 5391
publicaciones@themis.pe
www.themis.pe

Editores Generales
Daniel Masnjak M., Nuria Vega F. y Jordi Sardá P.

Editores
Óscar Lozada M., Isabo Hospinal A., Melissa Flores M., Alvaro Luna Victoria S.,
Henrry López J., Johanna Mosqueira G., Juan Alberto Liu S. y Rodrigo Roman O.

Diseño de portada: Renato Valdizán C., miembro de la Comisión de Imagen Institucional.

Diagramación: Mario Popuche Ll.

Hecho el Depósito Legal en la Biblioteca Nacional del Perú: N° 2019-10864
ISBN: 978-612-48087-0-8
1era edición, agosto 2019
Tiraje: 500 ejemplares

Editado por THĒMIS
Comisión de Publicaciones

Impreso en:
Litho & Arte S.A.C.
Jr. Iquique 026-Breña
Agosto - 2019

Sistemas de decisión automatizada en el sector público y protección de datos

Romina Garrido Iglesias*
Directora de Privacy Consulting

Introducción

Los derechos fundamentales constituyen un límite de respeto de la actuación entre los ciudadanos, y entre estos y el Estado. Deben ser garantizados, declarados y reconocidos, por este último, lo cual, implícitamente, significa contar con mecanismos de tutela efectiva. Dentro de este catálogo de derechos, encontramos los llamados derechos a la personalidad, entre los cuales se identifica en un primer momento a la vida, la integridad física, la salud, la honra, el honor y la privacidad.

Al surgir la informática, aparecen nuevos riesgos a los derechos fundamentales, con los cuales se cuestiona su concepción tradicional, en la medida que nuevas facetas de la personalidad humana se van desarrollando y, con ello, nuevos derechos se van configurando, como aquellos relacionados con los datos personales y su manejo automatizado o manual.

Las tecnologías de la información y las comunicaciones (en adelante las TIC) nos entregan la posibilidad de almacenar una enorme cantidad de información, luego de accederla y poder explotarla para infinitos usos. Del desarrollo de esas grandes bases de datos, surgen, por ende, riesgos por un eventual mal manejo de lo que se almacena en ellas. Esa información, sobre todo en áreas relevantes como la salud, la seguridad pública, la investigación científica, será muchas veces información referida a personas y será información sensible o especialmente protegida, cuyo procesamiento permitirá avances sociales importantes, pero cuya gestión merece un especial cuidado.

Siempre, desde la observación y análisis de datos, antes de manera manual, ha sido posible extraer conclusiones a diversos desafíos de la humanidad. Por eso, desde tiempos inmemoriales y hasta hoy, como parte de la instrucción de diversas profesiones como la estadística y la médica, asuntos tan importantes como el secreto y confidencialidad guían la relación entre datos y personas y son parte de la práctica de distintos oficios, no importa cuál sea el desarrollo o avance de la tecnología.

Hoy, enfrentamos un nuevo paradigma: son necesarias grandes cantidades de datos para el desarrollo de la humanidad, para una mejor salud, para espacios seguros, para la educación, para superar la pobreza. Los datos presentan una gran oportunidad de avances en el área sanitaria que nunca fueron imaginados. Las tecnologías de explotación masiva de datos y la Inteligencia Artificial (en adelante IA) nos están ayudando a resolver algunos de nuestros más grandes desafíos.

---

* Abogada y Licenciada en Ciencias Jurídicas de la Universidad de Valparaíso, Diplomada en Derecho Informático y Magíster en Derecho de las Nuevas Tecnologías por la Universidad de Chile. Certificada en Liderazgo y Estrategia en Ciberseguridad de la Universidad Internacional de Florida, Estados Unidos. Profesora del Diplomado de Ciberseguridad de la Facultad de Economía y Negocios en la Universidad de Chile, y profesora invitada deal Magíster de Informática Medica de la misma universidad. Colabora en la Red Iberoamericana de Protección de Datos, es fundadora de la ONG Datos Protegidos y de Privacy Consulting.

Pensemos, por ahora, en el área sanitaria. En Dinamarca, la IA está ayudando a salvar vidas al permitir que los servicios de emergencia diagnostiquen los paros cardíacos u otras condiciones basadas en el sonido de la voz de una persona que realiza una llamada. En Austria, está ayudando a los radiólogos a detectar tumores con mayor precisión al comparar instantáneamente los rayos X con una gran cantidad de otros datos médicos[1]. Estos son solo algunos ejemplos. De procesamiento manual, la investigación focalizada, la medicina hoy tiene la oportunidad de avanzar gracias a la posibilidad de explotar grandes bases de datos para el bien y para todos.

Estos datos, muchas veces, serán datos personales sensibles, los que, de ser incorrectamente manipulados, pueden producir efectos colaterales no deseados, desde la invasión a la privacidad, la vulneración de la confidencialidad médico-paciente, discriminaciones en el acceso a la salud y sesgos indeseados. La relación entre datos y personas necesita, entonces, una atención especial y ser protegida.

Este artículo reflexiona brevemente sobre las decisiones automatizadas, esto es tecnologías de procesamientos de datos que pretenden agilizar procesos, eliminar los sesgos humanos y otros los factores que, muchas veces, no son considerados por las personas.

En ningún caso, pretendemos abarcar aquí todas sus aplicaciones, sino entregar ciertos criterios jurídicos que apoyen su desarrollo y, sobre esa base, justificar su adopción. Todavía existe resistencia, en algunos casos, sobre aceptar o no la automatización, siempre por el riesgo de invasiones indeseadas al derecho a la privacidad. Son ya muchos los artículos sobre las ventajas de la aplicación de la inteligencia artificial y todos los problemas que promete solucionar; sin embargo, son pocas las reflexiones sobre sus aspectos legales y éticos que nos permitan vencer precisamente esa reticencia.

I. Decisión automatizada, inteligencia artificial, datos masivos. ¿Lo mismo?

Partiremos refiriéndonos a tres conceptos relacionados cuando pensamos en la decisión automatizada: la automatización propiamente tal como operación de tratamiento de datos; los datos necesarios para la posibilidad de generar dicha decisión, esto es, los datos masivos; y los algoritmos y la Inteligencia Artificial.

A. Automatización.

El profesor y matemático Alfred North Whitehead señaló que la "la civilización avanza extendiendo el número de operaciones importantes que podemos realizar sin pensar en ellas[2]". Esta es una didáctica forma de explicar que entendemos por la automatización de procesos.

El tratamiento de datos personales es una operación o un proceso "automatizable"; es posible que las operaciones de tratamiento, "las operaciones importantes", aquellas que han sido definidas en los cuerpos legales de protección de datos, como recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizar los datos en cualquier otra forma, se realicen por medio de máquinas "sin tener que pensar en ellas" mediante un algoritmo.

1 Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe. Disponible en https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe

2 https://www.theatlantic.com/education/archive/2015/11/math-showing-work/414924/

Cuando estos datos se refieren a una persona identificada o identificable, el sistema de decisión tendrá efectos significativos sobre ella, significa que el sistema necesita como insumo datos personales, y por tanto, la automatización merece nuestra atención. Ya en los albores de la computación, los legisladores advirtieron que las tecnologías podían usarse para socavar derechos de las personas: entre ellos, su privacidad. Desde ahí, se han erigido un conjunto de normativas y reglas sobre cómo deben ser tratados los datos personales, cómo protegerlos y cuáles son las salvaguardas de las personas frente a la automatización. Esto, pues, debemos entender que quien trata datos, su responsable o su controlador está tratando algo que es "de otro".

En Chile, tenemos una legislación que regula el tratamiento de datos, pero poco dice sobre la automatización. Pensemos que se trata de una legislación diseñada en los comienzos de internet. La Ley 19.628[3] de protección a la vida privada y que regula el tratamiento de datos personales, del año 1999, es una norma de aplicación general para toda actividad de tratamiento.

Esta ley se refiere, genéricamente, a que el tratamiento de datos puede ser o no de carácter automatizado, y que podrán establecerse procedimientos automatizados de transmisión de datos con ciertos requisitos. La ley no estableció garantías de control frente a las decisiones automatizadas cuando estas afecten a las personas o, dicho de otra forma, no estableció la capacidad o derecho de una persona de poder impugnarlas o refutarlas; esto es, a conocer que hay detrás y cómo se toma esta decisión. A esto nos referiremos más adelante.

B. Los datos masivos

Los datos son el componente central de todo sistema de decisiones automatizadas. Justamente, la clave de aquellos es que se alimentan con muchos datos: cuantos más datos, mejores decisiones o predicciones dicen los expertos. En efecto, la masividad es capaz de garantizar mejores decisiones, pues, mientras más datos les suministran, los sistemas son capaces de detectar mejores señales y aplicar mejores pautas[4].

Cuando hablamos de muchos datos para una mejor toma decisiones automatizadas, hablamos de sistemas que se alimentan del *Big Data*. Los datos masivos, "macrodatos", datos a gran escala o *Big data* –el anglicismo utilizado comúnmente–, se comprenden precisamente dentro de la ciencia de la computación llamada Inteligencia Artificial, o que en nuestro análisis le llamaremos la decisión automatizada. Las decisiones automatizadas precisan entonces de fórmulas matemáticas, estadísticas y datos, entre otros datos. Los datos, en estos sistemas, son el componente que enseña a estas máquinas a "pensar" como un ser humano[5]. Este proceso, no la decisión misma paro su ejecución, es delegada a un tercero, el que, a su vez, delega a la máquina, la que trabaja con un algoritmo. Cuando estos datos son personales, esto es se refieren a una persona identificada o identificable, como ya dijimos, su estatuto de protección es especial.

C. Algoritmos

Un algoritmo es una secuencia de comandos para que una computadora transforme un insumo en un resultado. Por ejemplo, una lista de personas se ordenará según su edad. La computadora toma las edades de las personas en la lista (insumo) y produce el nuevo ranking de la lista

3 Ley 19.628. En línea https://www.leychile.cl/Navegar?idNorma=141599

4 Mayer-Schönberger, V., & Cukier, K. (2013). Big data: la revolución de los datos masivos. Turner.

5 Mayer-Schönberger, V., & Cukier, K. (2013). Big data: la revolución de los datos masivos. Turner.

ordenada (resultado)[6]. En el área de las decisiones automatizadas, se utilizan varios algoritmos, que también podrían denominarse "formas de calcular las predicciones con el uso de datos"; muchos de estos algoritmos utilizan técnicas estadísticas para calcular la influencia de un conjunto de datos en un resultado seleccionado[7].

El uso esencial de los datos, en el campo de la toma decisiones automatizadas, son las predicciones. Una predicción puede definirse como el anuncio de un hecho futuro, ya sea por una "revelación", "conocimiento fundado" o "intuición o conjetura[8]". Las predicciones se consideran fundamentales entre las líneas estratégicas de investigación, por ejemplo, para la medicina. Resulta prometedor la posibilidad de predecir, mediante un sistema de decisiones automatizadas, cierto tipo de problemas médicos: el diagnóstico y el tratamiento de diversas enfermedades[9].

Con todo, no todos los algoritmos se usan para hacer predicciones. También se usan para hacer ajustes en procesos, para agilizar, para explicar y, con eso, tomar mejores decisiones de una política pública. El objetivo de un sistema de decisión automatizada puede ser, entonces, una predicción, explicación, o una agrupación de casos. En el desarrollo de modelos predictivos, se usan muchos algoritmos para, finalmente, definir cuál es el que más se acerca al resultado deseado. Crear algoritmos para hacer predicciones puede involucrar diferentes métodos, todos los cuales utilizarán datos para ser entrenados y de esa forma averiguar qué cálculos predicen un determinado resultado con mayor precisión[10].

D. Inteligencia artificial

Todos los debates hoy se centran en hablar de Inteligencia Artificial, pues el término "inteligencia" tiene connotaciones que son más comprensibles para nosotros, referidas a una autonomía e intencionalidad de tipo humano que, en este caso y para facilitar el entendimiento de todos, se atribuyen a las máquinas. Sin embargo, creemos que el término "decisiones automatizadas" define mejor lo que enfrentamos como sociedad que el término "Inteligencia Artificial"[11]. Un sistema de decisiones automatizadas son sistemas controlados algorítmicamente, en las que un proceso de decisión se delega parcial o totalmente a otro, el que a su vez toma o propone una decisión automáticamente.

Los sistemas de decisión automatizada son aquellos que, al analizar su entorno, realizan acciones con cierto grado de autonomía para lograr objetivos específicos. Estos pueden basarse exclusivamente en software, actuando en el mundo virtual (por ejemplo, asistentes de voz, software de análisis de imágenes, motores de búsqueda, sistemas de reconocimiento de voz y reconocimiento facial) o puede integrarse en dispositivos de hardware (por ejemplo, robots, automóviles autónomos, drones o dispositivos de internet de las cosas)[12].

---

6 European Union Agency for Fundamental Rights (2018) #BigData: Discrimination in data-supported decision making

7 European Union Agency for Fundamental Rights (2018) #BigData: Discrimination in data-supported decision making

8 Definición de la Real Academia Española.

9 Expósito Gallardo, M. D. C., & Ávila Ávila, R. (2008). Aplicaciones de la inteligencia artificial en la Medicina: perspectivas y problemas. Acimed, 17(5), 0-0.

10 European Union Agency for Fundamental Rights (2018) #BigData: Discrimination in data-supported decision making

11 Siguiendo las ideas del reporte de AlgorithmWatch & Bertelsmann Stiftung (2019) Automating Society Taking Stock of Automated Decision-Making in the EU. AW AlgorithmWatch gGmbH.

12 Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe. Disponible en https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe

Todos los días estamos usando estos sistemas, en un traductor en línea, en un filtro antispam, los cuales se alimentan de datos para optimizarse día a día.

E. La decisión automatizada como parte de las políticas públicas

En Chile, son diversas las iniciativas públicas de automatización de procesos y de incorporación de sistemas de inteligencia artificial basadas en algoritmos o decisiones automatizadas. La Superintendencia de Seguridad Social, órgano encargado del cumplimiento de la normativa de seguridad social de los trabajadores, pensionados y sus familias, se encuentra implementando un modelo de predicción de casos, reclamos y peticiones para agilizar los procedimientos administrativos de la ciudadanía[13]. El Ministerio de Salud, por su parte, explora, desde 2018, el uso, en los establecimientos públicos de salud, de un software de inteligencia artificial que permitirá al sistema de salud público detectar, con mayor precisión, anomalías asociadas a la retinopatía diabética, principal causa de pérdida de visión y ceguera en personas en edad laboral. El software analiza automáticamente los exámenes de retinopatía a través de un algoritmo que descarta cerca de un 80% de los casos que no presentan anomalías, optimizando los recursos en las pruebas con alteraciones, lo que permite hacer viable económica y temporalmente que otras personas con diabetes puedan acceder al examen anual[14].

También, en el mismo Ministerio, está en funcionamiento, desde febrero de 2019, el Sistema de Gestión de Pacientes con Enfoque de Riesgo para apoyar la priorización de las listas de espera. Se trata de un índice basado en un algoritmo que permite priorizar la posición de un paciente en lista de espera de acuerdo con su factor de riesgo, que se calcula en base a criterios clínicos. Es una herramienta de apoyo para que los médicos tomen una mejor decisión respecto al orden de atención de un paciente que, a su vez, está dentro de un grupo de personas que esperan por la misma patología o condición de consulta[15].

Un último ejemplo por mencionar es el que está en ejecución en el Ministerio de Desarrollo Social, el cual encargó el estudio y diseño de un predictor que pueda identificar, oportunamente, a los niños y niñas en situación de riesgo y prevenir situaciones de vulneración de sus derechos. A la fecha, se ha avanzado en la licitación de este sistema y se ha avanzado en la firma de convenios para la interoperabilidad de datos con otras instituciones y servicios públicos. Una vez detectados los casos mediante cruce de datos, es posible intervenir en las familias vulnerables, generar competencias, priorizar a niños en riesgo en la entrega de programas sociales, lograr una mayor eficiencia en la intervención y usar los recursos de manera inteligente, entre otros[16].

Y así, con el uso de esta tecnología en todos estos contextos, es posible analizar grandes cantidades de datos, más allá de toda capacidad humana, pues las personas no pueden considerar todas las posibilidades. No obstante las soluciones que ofrece un sistema de decisión automatizado, el sesgo -el no considerar todas las variables- puede terminar por introducirse de todas formas.

---

13 https://www.suseso.cl/605/w3-article-577921.html

14 Ministro de Salud presenta software que permitirá triplicar la cantidad de exámenes para prevenir la ceguera diabética. https://www.minsal.cl/ministro-de-salud-presenta-software-que-permitira-triplicar-la-cantidad-de-examenes-para-prevenir-la-ceguera-diabetica/

15 Minsal presenta Sistema de Gestión de Pacientes con Enfoque de Riesgo para apoyar priorización de las listas de espera https://www.minsal.cl/minsal-presenta-sistema-de-gestion-de-pacientes-con-enfoque-de-riesgo-para-apoyar-priorizacion-de-las-listas-de-espera/

16 http://losninosprimero.cumplimiento.gob.cl/alerta-ninez.html y http://www.economiaynegocios.cl/noticias/noticias.asp?id=504409

Los ejemplos que mencionamos anteriormente son ya una realidad. Sin embargo, para algunos, no está muy claro que el Estado pueda incorporar este tipo de tecnologías en sus procesos y cuestionan tanto la decisión misma y su autonomía frente a la decisión que tradicionalmente tomaba un funcionario público, como también las salvaguardas legales y éticas respecto del tratamiento de esos datos ajustado a las normas que rigen sus competencias. El análisis normativo de competencias y obligaciones que se adquieren, por el tratamiento de datos, es una cuestión previa frente a cualquier implementación de tecnología en ese sentido.

Aprovechar los datos puede resultar muy beneficioso, pues nos permite resolver problemas urgentes. Sin embargo, estos datos muchas veces serán sensibles: datos de salud, datos de menores, datos de la seguridad social, especialmente protegidos produciéndose una situación paradojal respecto de su protección, pues, justamente, bajo estas lógicas de negocio, todo está diseñado para "compartir" lo que, aparentemente, es contrario a proteger.

Cuando pensamos en la automatización, entonces no se trata solo reglas seguidas por máquinas, sino que hay también un proceso previo de recopilación, preparación y análisis previo al desarrollo técnico. Toda la etapa de objetivos, necesidades, variables son parte de un proceso humano y, como todo proceso humano, puede tener sesgos. No debemos olvidar que las nuevas tecnologías se basan en valores, en intenciones. La implementación de toda tecnología transformadora, como la decisión automatizada, puede plantear nuevas cuestiones éticas y legales; por ejemplo, quién tiene la responsabilidad final de la decisión, cuál es la fuente de los datos, o la toma de decisiones potencialmente sesgada.

En ese contexto, el Estado, entonces, no solo debe garantizar el bien público como fin último, sino que debe conciliar que los sistemas se desarrollen y apliquen en un marco adecuado que promueva la innovación y respete los derechos fundamentales de quienes va dirigido; esto es considerar una serie de reglas respecto de la forma de tratar la información que alimentan estos sistemas, sus datos personales, para que el enfoque de las políticas públicas realmente beneficie a las personas, y la sociedad, en general, necesita observar esas reglas[17].

F. Protección de datos personales

Las normas de un adecuado tratamiento de datos personales deben formar parte de todo sistema de decisión automatizada. Los datos personales y la privacidad se clasifican dentro de la tipología de riesgos que las organizaciones deben abordar en los contextos de proyectos de automatización, *big data* y algoritmos, pues se trata de sistemas que hacen un uso intensivo de datos. Este es un tema no menor, pues ya muchos han enfatizado en la manera que estos sistemas pueden, fácilmente, dar un giro hacia la vigilancia masiva con graves efectos sobre los derechos de las personas[18].

Las reglas de protección de datos son la forma de garantizar la licitud, calidad de datos, la responsabilidad y la transparencia del tratamiento masivo de datos que realizan los sistemas de decisión. Pensemos que el tratamiento de datos de estos sistemas, casi siempre, constituirá un uso distinto para el cual fueron recopilados en un primer momento. Los datos pasan de ser de una fuente primaria a otra secundaria volviéndose mucho más valiosos. Veremos, a continuación, cuáles son esas reglas de protección.

17 Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe. Disponible en https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe

18 Buenadicha, C., Galdon, G., Hermosilla, M. P., Loewe, D., & Pombo, C. (2019). La gestión ética de los datos.

1. Antecedentes

Diversos países, incluido Chile, Perú, Colombia, Argentina, Uruguay, Costa Rica, por mencionar algunos, han reconocido, en sus leyes y Constituciones, una garantía explícita de resguardo a los datos personales, entregando a las personas su control en los entornos físicos y digitales ante la potencialidad de cruzar información, transmitirla, alterarla, eliminarla y efectuar diversas operaciones. Estas leyes otorgan diversos grados de protección y la reconocen con diversos grados de autonomía.

En Chile, el derecho a la protección de datos está reconocido constitucionalmente desde junio de 2018, mediante una modificación al artículo 19 numeral 4, incorporándolo al mismo nivel del derecho a la privacidad, pero como derecho autónomo. En la práctica, este cambio implica que será posible acudir por la vía constitucional, esto es por "recurso de protección de garantías constitucionales", no solo por la infracción de los derechos de acceso, rectificación, cancelación y oposición, sino también por la infracción a principios y reglas del tratamiento fijadas en la ley: calidad, finalidad, diligencia, confidencialidad.

La protección de datos es la *facultad de control* sobre los datos frente a su tratamiento automatizado o no. Este control presenta una triple faceta. Primero, reconociendo capacidades en las personas; esto es el reconocimiento de derechos. Segundo, mediante los principios y reglas del tratamiento; y, tercero, los controles institucionales. Los controles institucionales pueden ejercerse través de autoridades públicas de control con facultades de fiscalización, supervisión e intervención sobre quienes tratan datos mediante mecanismos de autocontrol y a través de mecanismos de control interno en las organizaciones; por ejemplo, un rol específico dentro de la organización que vele por el cumplimiento normativo, conocido como oficial de privacidad o encargado de protección de datos.

2. Las reglas de tratamiento

El tratamiento de datos es una actividad permitida, pero estrictamente regulada. Los datos personales pueden ser datos genéricos de mera identificación o datos sensibles, que cuentan, por tanto, con una protección superior objetiva. Los datos sensibles son aquellos datos personales que se refieren a las características físicas o morales de las personas, o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual[19].

En la actualidad, las leyes de protección de datos se refieren a los datos sensibles también como una categoría distinta o particular de datos personales, llamándolos datos especialmente protegidos. Cualquiera sea la nomenclatura, el contenido del dato es lo que finalmente justifica un tratamiento especial. Una adecuada protección de datos debe permitir el control en el tratamiento de todos los datos, esto es un tratamiento con las debidas garantías para no lesionar la dignidad y libertad de las personas.

El dato sensible es un tipo de dato personal. No es intrascendente que señalemos esto, debido a que, muchas veces, se confunde qué es lo que se debe efectivamente proteger. Las leyes de protección de datos deben garantizar la disposición de los individuos sobre todos sus datos personales y personales-sensibles, impidiendo que estos se conviertan en fuentes de información

19 Ley Nª 19.628 Art. 2 letra G http://www.leychile.cl/Navegar?idLey=19628

sin las debidas garantías. También, los cuerpos normativos deben ser eficaces para prevenir todo tipo de riesgos que puedan derivarse de su tratamiento, divulgación o acceso indebido.

Diremos, entonces, que son datos personales sensibles cualquier información que pueda dar origen a una "discriminación ilegal o arbitraria o conllevar un riesgo grave para el interesado"[20]. Pueden existir diferencias entre distintas legislaciones sobre cuáles de los datos son o no sensibles; sin embargo, hay un general consenso en que los datos de menores, de salud, los datos biométricos, son datos sensibles.

El dato sensible en Chile tiene una prohibición general de tratamiento, salvo que la ley autorice –existencia de competencias legales públicas–, se cuente con el consentimiento informado y por escrito del titular de los datos o, no existiendo ninguno de los supuestos anteriores, que de su tratamiento derive de un beneficio de salud para su titular. El escenario es bastante restringido respecto a cómo se ha regulado esta cuestión en normativas como el Reglamento Europeo de Protección de Datos, en el cual se reconocen otras habilitantes para el tratamiento de datos especialmente protegidos, como lo será el interés vital y el interés público, en algunos casos.

La habilitación legal para tratar diversas fuentes de datos, basado en un interés público, no significa inobservancia de reglas. Estas reglas están, en diversos cuerpos normativos, de cada ente público respecto de sus competencias según dispone el artículo 20 de la Ley 19.628, pues el tratamiento de datos personales, por parte de un organismo público, solo podrá efectuarse respecto de las materias de su competencia, en cumplimiento de sus funciones legales, y con sujeción a las reglas de protección de datos. En esas condiciones, no necesitará el consentimiento del titular. Actualmente, no hay mayor mención acerca de las responsabilidades y también de las capacidades de un órgano público para tratar datos.

El proyecto de ley actualmente en discusión, en el Senado a abril de 2019, complementa lo anterior y dispone, además, que el tratamiento de los datos personales que realicen los órganos públicos se rige por los principios establecidos en el artículo 3° y los principios de coordinación, eficiencia, transparencia y publicidad.

En virtud del principio de coordinación, los organismos públicos deben alcanzar un alto grado de interoperabilidad y coherencia, de modo que se evite contradicciones en la información almacenada y reiteración de requerimientos de información o documentos a los titulares de datos. Conforme al principio de eficiencia, se debe evitar la duplicación de procedimientos y trámites entre los organismos públicos, y entre éstos y los titulares de la información. De acuerdo con los principios de transparencia y publicidad, los organismos públicos deben dar acceso a la información que tengan a su disposición, resguardando las funciones fiscalizadoras e inspectoras y los derechos de las personas que pudieran verse afectadas por ello[21].

Asimismo, se regulan las cesiones de datos, cuestión que hoy en día ocurre, pero queda a la discreción de cada organismo entregar un mayor o nivel de protección.

20 Véase la Resolución de Madrid, documento conjunto elaborado por diversas autoridades de protección de datos en la defensa y la mejora de la privacidad e información personal, con el objetivo de uniformar criterios de aplicación independiente de los modelos existentes de protección de datos y privacidad. Esta Resolución fue objeto del trabajo de los garantes de protección de datos el año 2009 en el contexto de la 31ª Conferencia Internacional de Autoridades Protección de Datos y Privacidad, teniendo como coordinador de este trabajo a la Agencia Española de Protección de Datos.

21 Artículo 23 nuevo propuesto. Boletines refundidos 11092-07 y 11144-07 actualmente en el Senado de Chile.

En cuanto a las directrices o reglas de la ley 19.628[22], sobre protección a la vida privada, esta norma obliga a los entes públicos a considerar a lo menos lo siguiente:

- La naturaleza jurídica del dato sensible, artículo 2 letra g) de la ley.
- La existencia de una legitimación para el tratamiento, por aplicación del artículo 10, basada en la ley que autoriza el tratamiento de datos por competencias.
- Las normas sobre finalidad del tratamiento, responsabilidad y confidencialidad de los artículos 4°,7° y 9°.
- La normativa sobre transmisión automatizada de datos y registros mínimos de auditabilidad, contenida en el artículo 5°.
- Las reglas de debida diligencia, donde se incluye la seguridad, artículo 11°.
- La posibilidad de un tratamiento por encargo o mandato, artículo 8°.
- La obligación de cautelar los denominados derechos ARCO (acceso rectificación, cancelación y oposición), según dispone su artículo 12°.

3. Los usos secundarios

Como ya adelantamos, la explotación de los datos obtenidos de las fuentes de datos cedidas o como fruto de la recolección propia, para un sistema de decisiones automatizadas, tendrá siempre un objetivo distinto de aquel que motivó la recogida. La finalidad primaria o autorizada por las competencias legales es tratar los datos para una finalidad específica. Su explotación, posterior, en un sistema de inteligencia artificial o de *big data*, constituye un uso secundario de la información y, por ende, un nuevo tratamiento. En efecto, ya no se está usando el dato para la finalidad declarada, sino que la información de esa persona alimenta una gran masa de datos.

No existe una norma, en Chile, que se refiera a los usos secundarios. Por el contrario, se consagra un principio de finalidad estricto, y no permite excepciones a la prohibición de tratar categorías sensibles de datos para usos secundarios, como sí se señala expresamente en la normativa europea de tratamiento de datos, el Reglamento Europeo de Protección de Datos[23] (GDPR, por sus siglas en inglés). Esta normativa considera diversas habilitantes para el tratamiento, distintas del consentimiento y la ley, incluidas las razones de interés público, la sanidad pública y el interés vital.

No obstante la falta de norma local expresa, la posibilidad de un uso secundario debe, necesariamente, basarse en objetivos de política pública, la que podrá justificarse en razones de existencia de un interés legítimo y amparado en una obligación legal (sus funciones), en la medida que la autoridad cumpla con todos y cada uno de los principios y normas rectoras del tratamiento de datos personales, y actúe dentro de la órbita de sus competencias. Esto, pues el uso secundario de los datos es un nuevo tratamiento, el cual debe observar ciertas pautas. Un uso secundario de los datos se estima suficientemente justificado en las facultades de formular, fijar y controlar las políticas públicas de un sector, como parte del interés público, siempre y cuando se adopten garantías suficientes y adecuadas.

Como ya señalamos, en Chile, la ley autoriza el tratamiento de datos personales, por parte de un organismo público, respecto de los asuntos de su competencia y con sujeción a

22 Ley 19.628.

23 Disponible en https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:32016R0679

las reglas de la Ley 19.628 como un mínimo. En esas condiciones, no necesitará el consentimiento del titular[24]. Para algunos, estas competencias deben estar explícitamente en la ley orgánica del organismo público.[25] Sin embargo, creemos que, si bien no se trata de justificar "competencias genéricas" a una autoridad administrativa, es preciso conciliar, por un lado, el desarrollo de la tecnología y sus ventajas, y los objetivos del órgano público en el sentido que se ha interpretado en Europa. No necesariamente la obligación jurídica de tratar datos existe, pero el tratamiento es necesario para el ejercicio de dicha potestad[26]. Si bien todo tratamiento de datos puede afectar en menor o mayor medida garantías constitucionales, es necesario establecer las salvaguardas suficientes para un procesamiento racional y justo. La ausencia de una autoridad de control, para fijar requisitos materiales de las actividades de tratamiento, complica aún más el camino y transforma la actividad de tratamiento en una asunto aún más riesgoso, pues debemos dilucidar cuándo estamos frente a una obligación jurídica que se cumple tratando datos.

Junto con mencionar el uso secundario de datos como una parte que debemos considerar dentro de un sistema de decisión automatizada, es importante focalizar la atención en la decisión misma y su ejecución, la cual estará basada en un algoritmo de aprendizaje automático. El proceso de aprendizaje, si bien necesita grandes cantidades de datos para desarrollarse, también es un proceso matemático distinto del dato mismo.

G. Las decisiones automatizadas y protección de datos. Hacia un sistema de responsabilidad

En la era de la automatización, ya no resultan suficientes las categorías tradicionales de protección de datos para asegurar su debido resguardo. Por ejemplo, la exigencia del consentimiento como única base jurídica para cualquier tratamiento de datos automatizado o no.

Hoy, estas transmisiones automáticas ocurren a cada momento y un sistema de notificación-consentimiento resulta inútil y molesto, e igualmente inútiles las autorizaciones genéricas para el uso de datos en otros procesos distintos al de la recolección, y en algunos casos incluso no son suficientes las técnicas de anonimización[27]. Respecto de esto último, no existen sistemas completamente infalibles que garanticen el total anonimato.

No queremos decir que el consentimiento y la anonimización no deben aplicarse en la decisión automatizada, estos deben aplicarse siempre que sea posible para disminuir aún más los riesgos sobre las personas. El asunto es que hoy son tantas las fuentes que capturan nuestros datos, como tantas las fuentes disponibles para el que los desea explotar. Por otra parte, la anonimización irreversible no es posible. Si pensamos, por ejemplo, en el área sanitaria, donde muchas veces el proceso adecuado, para usar ese dato, es la pseudonimización o reemplazo de ciertos atributos que dificulten a primera vista la identificación, esta debe ser reversible siempre que sea posible.

En Chile, las decisiones automatizadas no están reguladas de manera cabal. La ley señala que el tratamiento puede ser automatizado o no y que el responsable del registro o banco de

24 Artículo 20 ley 19.628.

25 Una postura en ese sentido en Vega, L. C. (2008). Videovigilancia e intervención administrativa: las cuestiones de legitimidad. Revista de Derecho Público, (70), ágs-359.

26 Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos (WP 217)

27 Opinion 05/2014 on Anonymisation Techniques. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

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[28].

La ley fija algunos mínimos frente a un requerimiento de datos personales mediante una red electrónica, donde el responsable de los datos deberá dejar constancia de lo siguiente:

a) La individualización del requirente.

b) El motivo y el propósito del requerimiento.

c) El tipo de datos que se transmiten.

La admisibilidad del requerimiento de transmisión de datos deberá ser evaluada por el responsable del banco de datos que recibe la petición, pero la responsabilidad, por dicha petición, será de quien la haga. Los datos solo pueden utilizarse para los fines que motivaron la transmisión.

Esta disposición es aplicable, entonces, tanto para transferencias o cesiones de datos, como para transmisiones de, datos y básicamente, consagra que el responsable debe dejar pistas de auditabilidad o trazabilidad para cuando los datos se comparten electrónicamente y de manera automatizada.

Junto con el deber del responsable de resguardar ciertos mínimos en la automatización, las legislaciones de protección de datos reconocen el derecho de toda persona a no ser objeto de una decisión basada únicamente en el tratamiento automatizado (como, por ejemplo, un algoritmo) y que sea jurídicamente vinculante o que les afecte significativamente. Con ello, también se garantiza el derecho a impugnarla.

Una decisión *produce efectos jurídicos* cuando se vean afectados los derechos de una persona; por ejemplo, el acceder o no a una atención de salud mediante un algoritmo de priorización de espera, que no tiene intervención humana alguna. La decisión debe contener algún tipo de intervención humana y no ser únicamente automática. Una decisión *afecta significativamente* a una persona si esta influye en las circunstancias de la persona, su comportamiento o sus decisiones de manera negativa[29].

Creemos que lo que debe implementarse, para los procesos de decisión automatizada, es un sistema basado en la posibilidad de demostrar que el dato se trata siguiendo ciertas pautas de cuidado o responsabilidad. Este sistema de responsabilidad debe considerar, a lo menos, lo siguiente:

1. Una base legal

En términos generales, todo tratamiento de datos debe contar con una base jurídica suficiente o una habilitante del tratamiento que lo justifique. Estas habilitantes se resumen en lo siguiente:

– El consentimiento.

– El contrato.

– El cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento.

28 Ley 19.628, artículo 5° de la Ley 19.628.

29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)

– El interés vital del interesado.
– El interés público.
– El interés legítimo.

Respecto de ellas, diremos que ninguna de estas habilitantes se prefiere una a otra, y debemos, también, señalar que "los intereses" que habilitan un tratamiento requieren siempre un análisis de "necesidad." De todos ellos, el interés legítimo resulta el más polémico de todos y, muchas veces, el más difuso[30].

Sobre el interés vital como un habilitante para el tratamiento de datos, resultan conflictivos aquellos casos en que se pretende utilizar esta habilitante para el tratamiento de datos a gran escala o en aquellos casos en que obtener el consentimiento resulta desproporcionado. El interés vital no es necesariamente individual y aislado; sin embargo, no puede justificarse el tratamiento masivo, únicamente, en el interés vital. Para otros usos relacionados con intereses esenciales de la vida del titular que no sean inmediatos, el consentimiento deberá solicitarse siempre que sea posible. No obstante, el interés vital podría querer abarcar cierto tipo de procesamiento por importantes razones de interés público; por ejemplo, automatización para desarrollar modelos que predicen la propagación de enfermedades que amenazan la vida o en situaciones de emergencia humanitaria. En estos casos, el interés legítimo puede ser base legal suficiente.[31]

Complementando lo anterior, las decisiones automatizadas para fines, por ejemplo de perfilamiento automatizado, las autoridades europeas las han estimado permitidas cuando se cumpla alguno de los siguientes supuestos[32]:

– Una ley expresamente permite la decisión automatizada, y derechamente por ejemplo el uso de algoritmos. El uso de la automatización, por ejemplo, es parte de una obligación jurídica del responsable.
– La persona ha consentido explícitamente una decisión basada en el algoritmo.
– La decisión basada en el algoritmo es *necesaria* (es decir, no puede existir otra forma de alcanzar el mismo objetivo), por ejemplo, para celebrar o ejecutar un contrato con la persona cuyos datos haya tratado a través del algoritmo (por ejemplo, una solicitud de préstamo por internet), acá también cae la categoría del interés público comprometido o responde a razones de interés vital o el interés legítimo.

Especial atención merece si la automatización utiliza categorías especiales de datos personales o datos sensibles, donde las decisiones que ejecute solo estarán permitidas cuando se cumplan alguno de los siguientes supuestos:

– Consentimiento expreso de la persona.
– Existencia de un interés público comprometido, esto es, la decisión es necesaria para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento. En esta situación se encuentran los responsables que tienen una potestad pública

30 Puede revisarse el Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos (WP 217)

31 Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos (WP 217)

32 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)

o una misión de interés público (pero no necesariamente una obligación jurídica de tratar los datos) y el tratamiento es necesario para el ejercicio de dicha potestad[33].

Respecto del consentimiento, es decir, tener la opción de manifestar las posibilidades o no del uso de la información personal cuando ha sido obtenida de un titular, los sistemas de privacidad tradicionales plantean que la persona debiese ser capaz de elegir si quiere que su información alimente o no una masa de datos para uso secundario. Estos sistemas de notificación se tornan ineficaces cuando se trata de cláusulas, en los documentos informativos, donde se autoriza cualquier uso posterior de manera genérica. Este sistema centrado, aparentemente, en la voluntad de la persona no es tal, puesto que estas cláusulas no consideran, en el fondo, algún tipo de responsabilidad del tratador, limitación de la finalidad, y, además, socavan gravemente objetivos importantes que se logran con el tratamiento de datos[34].

II. Finalidad

Señalábamos que en la mayoría, sino todas las veces, el tratamiento de datos, en los contextos de sistemas de decisiones automatizadas, será un tratamiento secundario, donde resulta indispensable justificar, entonces, su base legal de cara a la finalidad. En efecto, las bases legales que mencionamos deben analizarse desde la óptica de un uso secundario, esto es una base legal distinta de aquella considerada en la recolección del dato y primer uso. Como ya dijimos, un sistema de decisión automatizada no está usando el dato para la finalidad declarada en un principio, sino que la información de esa persona alimenta una gran masa de datos.

Para lo anterior, conviene, entonces, determinar lo siguiente:

- La relación entre los fines para los que se han recopilado los datos y los fines del tratamiento secundario. Por ejemplo, fines igualmente sanitarios, fines de seguridad social, fines que igualmente contribuyen al interés vital de la persona, etc.
- El contexto en el que se recopilaron los datos y las expectativas razonables de las personas respecto de un posible uso secundario.
- La naturaleza de los datos en cuanto a su uso posterior y su impacto en los titulares. Esto se vincula con la clase de garantías a implementar.
- Las medidas de seguridad aplicadas por el responsable para garantizar un procesamiento justo y para evitar cualquier uso indebido.

En el procesamiento de datos para el *big data* o la Inteligencia artificial, no resulta suficiente las cláusulas genéricas en la recolección del dato, donde el titular autoriza un uso futuro e indeterminado para cumplir con el requisito legal de la "finalidad informada", como lo señalamos cuando mencionamos el consentimiento como base legal. Los sistemas de decisión automatizada nos obligan abordar esta cuestión más allá de la "privacidad por consentimiento" y avanzar a la "privacidad por responsabilidad[35]", que es justamente el enfoque de las normativas europeas, que establecen requisitos de garantías adecuadas; esto es medidas de transparencia, información y certificación de procesos para aquellos que tratan datos.

33 Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos (WP 217)

34 Etzioni, A. (2010). Los límites a la privacidad.

35 Mayer-Schönberger, V., & Cukier, K. (2013). Big data: la revolución de los datos masivos. Turner.

III. Garantías adecuadas

Las garantías adecuadas aparecen, reiteradas veces, como un requisito de tratamiento en el contexto del Reglamento Europeo de Protección de Datos. Se refieren a todas las medidas de protección que puede tomar un responsable frente al tratamiento de datos automatizado, tanto en la operación de tratamiento original, como en la operación de tratamiento ulterior prevista.

El Reglamento señala que las garantías adecuadas:

> "Pueden consistir en normas corporativas vinculantes, cláusulas tipo de protección de datos adoptados por la Comisión Europea o por una autoridad de control, o a cláusulas contractuales autorizadas por una autoridad de control. Esas garantías deben asegurar la observancia de requisitos de protección de datos y derechos de los interesados adecuados al tratamiento, incluido los derechos exigibles y de acciones legales efectivas, de reparación administrativa o judicial cuando corresponda. En particular, deben referirse al cumplimiento de los principios generales relativos al tratamiento de los datos personales y los principios de la protección de datos desde el diseño y por defecto"[36].

Estas serán necesarias en caso de usos secundarios, tratamiento de datos a gran escala y todo aquel que pueda entrañar algún riesgo mayor para los titulares de datos. El responsable asume una mayor carga debido al uso distinto de los datos y la justificación de una nueva base legal. Las garantías adecuadas son medidas demostrables, pueden ir desde la diligencia debida al contratar, por ejemplo, estableciendo mayores exigencias a terceros encargados de desarrollos y tratamientos, hasta implementar mecanismos eficaces que permitan a los titulares ejercer su derecho de oponerse al tratamiento.

Las garantías adecuadas, en las legislaciones que cuentan con autoridades de control, son muchas veces fijadas o recomendadas por la autoridad de datos personales, generalmente en contextos de tratamiento de alto riesgo, categorías de datos sensibles y cuando las habilitantes se basen en algún tipo de "interés", esto es, no existe una habilitación legal expresa para tratar los datos, pero si puede existir una necesidad. De esta forma, la autoridad sopesa los derechos de las personas que ceden en virtud de dicho interés y fija algunos parámetros.

La propuesta es que, dentro de las garantías adecuadas para un sistema de decisión automatizada basado en tratamiento de datos personales, puedan incorporarse, además, los principios de responsabilidad de los algoritmos[37], que han sido consensuados por la comunidad científica. Como veremos, estos principios encuentran una estrecha relación con la protección de los datos y su gestión ética, y pueden ser esos mecanismos, que bajo la autonomía de la voluntad contractual o unilateral del responsable, puede proactivamente adoptar.

– El responsable de los datos es también responsable de las decisiones automatizadas, tomadas por sus sistemas, por ejemplo, por los algoritmos que ellos usan, incluso si no es capaz de explicar en detalle cómo los algoritmos producen sus resultados. Si la decisión forma parte de un proceso llevado por una autoridad pública, esta debe ser capaz de explicar los procedimientos seguidos por el sistema y, en particular, de la forma en que se toma la decisión. La responsabilidad de las decisiones debe recaer en las personas y en las instituciones, y no en el algoritmo mismo[38].

36 Considerando 108, Reglamento (ue) 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016.

37 http://www.fatml.org/resources/principles-for-accountable-algorithms

38 Buenadicha, C., Galdon, G., Hermosilla, M. P., Loewe, D., & Pombo, C. (2019). La gestión ética de los datos.

– El responsable debe ser capaz de garantizar la forma en que se recopilaron los datos, y su procedencia lícita. Esto servirá para poder determinar la posibilidad de sesgos potenciales, inducido por el proceso de recopilación de datos. Acá, es relevante considerar el principio de calidad de los datos, en cuanto a que recae en el controlador garantizar que el dato es exacto, adecuado, pertinente, veraz y no excesivo.
– Los modelos, algoritmos, datos y decisiones se deben registrar para poder auditarlos. Para esto, las instituciones deben usar métodos rigurosos para validar sus modelos y documentar esos métodos y resultados. En particular, deben realizar rutinariamente pruebas para evaluar y determinar si el modelo genera daño discriminatorio. Estas pruebas y auditorias deben transparentarse[39].
– Es recomendable –y en algunos casos obligatorio– realizar el proceso de evaluación de impacto en la protección de datos, el que se explicará más adelante.
– Las instituciones públicas que externalicen desarrollos, sistemas o servicios de decisión automatizada, a un encargado del tratamiento, deben exigir contractualmente un respaldo económico suficiente por el uso indebido de los datos o las vulnerabilidades de seguridad que pudieran producirse, prohibir expresamente las finalidades distintas, regular extensamente la destrucción posterior y los asuntos relativos al almacenamiento, responsabilidad de sus empleados o dependientes, incluida toda la cadena de subcontratación, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo.
– La seguridad sobre los datos personales. Las garantías adecuadas deben asegurar que se aplican medidas técnicas y organizativas para que se observe, en particular, el principio seguridad y el de minimización de los datos, incluida la existencia de mecanismos de cifrado o la seudonimización.

IV. Información

El derecho a la información es fundamental para garantizar la transparencia de los sistemas de decisión automatizada. La información forma también parte de las garantías adecuadas. Lo mínimo a informar respecto de un sistema de decisión automatizada es lo siguiente:

– La lógica aplicada en el proceso de toma de decisiones.
– Explicar de forma clara y sencilla cómo funciona el proceso de toma de decisiones automatizada.
– El derecho a obtener intervención humana.
– Las posibles consecuencias del tratamiento.
– Los mecanismos de impugnación.

V. La impugnación

El derecho a impugnar la decisión automatizada es el derecho a refutarla, es decir, a oponerse y tener el derecho a conocer aquellos factores que influyen en la decisión. No basta con la consagración del derecho a impugnar, pues deberán existir procedimientos accesibles para que la persona pueda expresar su punto de vista y conocer la forma en que se toma esa decisión. El derecho a la impugnación no está reconocido en Chile en términos generales, sino solo respecto a la posibilidad de impugnar una decisión que afecte a una persona en sus datos de

39 http://www.fatml.org/resources/principles-for-accountable-algorithms

carácter comercial y económico, pero no en todos los casos[40]. Una reforma legislativa se tramita actualmente en este sentido, reconociendo el derecho a la impugnación de las valoraciones personales como un nuevo derecho de las personas frente a la decisión automatizada.

Esta reforma considera, en términos generales, que el titular de datos tiene derecho a oponerse a que el responsable adopte decisiones que le conciernan, basadas únicamente en el hecho de realizarse a través de un tratamiento automatizado de sus datos personales, incluida la elaboración de perfiles, con excepción de un procesamiento de datos basado en el contrato, el consentimiento y la ley. También, se consagra que el titular siempre tiene derecho a obtener intervención humana del responsable, a expresar su punto de vista y solicitar la revisión de la decisión[41].

Las recomendaciones respecto a cómo el responsable lo es también de garantizar la impugnación desarrolladas por las autoridades europeas de protección de datos son las siguientes[42]:

- Es un derecho que opera en todos los casos.
- Debe ofrecerse de manera separada al derecho general de información.
- Ejercido el derecho, el responsable debe interrumpir o evitar iniciar el procesamiento de datos, al menos respecto del titular que lo ejerce. Sin embargo, existirán casos en que el responsable deberá demostrar que la decisión es beneficiosa para la sociedad en general, por ejemplo, para la investigación científica o predecir la propagación de enfermedades o apoyar en su diagnóstico. El único tratamiento esencialmente impugnable y donde el titular tiene un derecho sin condiciones es objetar el procesamiento de sus datos personales para fines de marketing directo.
- Respecto a la carga probatoria, esta recae en el responsable quien deberá demostrar: (i) que el impacto en los datos es mínimo, y que se han tomado medidas para atenuar un posible daño o riesgo a la privacidad tales como la anonimización o la pseudonimización de datos, garantizando de esa manera un procesamiento lo menos intrusivo posible; y (ii) que la decisión automatizada no solo es eficiente, sino que también responde a un objetivo crítico de la organización.

VI. La evaluación de impacto en protección de datos

Finalmente, y, sin querer ahondar en este punto donde el lector podrá encontrar manuales y guías específicas desarrolladas por las autoridades de control y grupos de trabajo europeos de protección de datos e inclusive estándares ISO[43], es recomendable, dada la complejidad del proceso de toma de decisiones automatizada, realizar una evaluación de impacto en la protección de datos, previa a cualquier implementación.

Una evaluación de impacto es un proceso concebido para describir el tratamiento, evaluar su necesidad y proporcionalidad y ayudar a gestionar los riesgos para los derechos y libertades

40 Artículo 9° inciso 3° ley 19.628: "Prohíbese la realización de todo tipo de predicciones o evaluaciones de riesgo comercial que no estén basadas únicamente en información objetiva relativa a las morosidades o protestos de las personas naturales o jurídicas de las cuales se informa. La infracción a esta prohibición obligará a la eliminación inmediata de dicha información por parte del responsable de la base de datos y dará lugar a la indemnización de perjuicios que corresponda".

41 Artículo 8° bis nuevo Boletines refundidos 11092-07 y 11144-07 actualmente en el Senado de Chile.

42 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)

43 ISO/IEC 29134:2017(en) Information technology - Security techniques - Guidelines for privacy impact assessment.

de las personas físicas derivados del tratamiento de datos personales, evaluándolos y determinando las medidas para abordarlos[44]. Las evaluación de impacto está conformado por instrumentos importantes para la rendición de cuentas, pero también para la gestión de los datos, ya que ayudan a los responsables no solo a cumplir los requisitos normativos, sino también son un elemento fundamental para la rendición de cuentas.

En Europa, son obligatorias, por disposición del Reglamento Europeo de Protección de Datos, artículo 35, cuando se trate de sistemas de evaluación sistemática y exhaustiva de aspectos personales de una persona, incluida la elaboración de perfiles cuando el tratamiento sea a gran escala de datos sensibles, o cuando el tratamiento contemple la observación sistemática a gran escala de una zona pública.

En Estados Unidos, estas evaluaciones son obligatorias para las agencias federales gubernamentales desde 2002 y están contenidas en la sección 208 de la Ley de Gobierno electrónico[45]. Estas evaluaciones importan análisis para asegurar la conformidad con los requisitos legales, regulatorios y de políticas aplicables para la privacidad de los datos, determinar los riesgos y evaluar protecciones y procesos alternativos para mitigar los posibles riesgos de privacidad.

VII. Conclusiones

Como parte de la instrucción de diversas profesiones y actividades, el secreto y confidencialidad guían la relación entre datos y personas, y son parte de la práctica de distintos oficios, no importa cuál sea el desarrollo o avance de la tecnología. Pensemos en la estadística, en la medicina, la abogacía, las finanzas. Sin embargo, en el desarrollo de disciplinas vinculadas a la ciencia de los datos, es algo muy incipiente, pero sumamente necesario para garantizar que los sistemas no se vuelvan contra las personas a quienes buscan beneficiar.

La automatización, por tanto, debe incorporar las consideraciones mínimas de protección de datos que hemos señalado, reconociendo la capacidad en las personas de poder informarse sobre la existencia de estos procesos y cuáles son las formas de poder ejercer sus derechos respecto de ellos o cuál han sido las medidas proactivas de transparencia adoptadas por el responsable.

Los conceptos de decisión automatizada o inteligencia artificial, datos masivos, algoritmos, están entre si relacionados: las decisiones automatizadas necesitan de datos y, mientras mayor cantidad de éstos se dispongan, más aún entrena el algoritmo bajo la promesa que serán mejores las decisiones. La automatización de esas decisiones, mediante el procesamiento de datos, merece la atención sobre todo en las áreas sensibles, como la observación de personas a gran escala, el uso de sistemas biométricos y el área sanitaria, por mencionar algunos.

La protección de datos, en el área de la explotación masiva de datos, para servir a intereses comunes como por ejemplo la salud, la seguridad pública u otros, está llena de anomalías. Se produce un claro desequilibrio, pues se inclina hacia el lado de servir a un bien común importante por sobre aquellas garantías de confidencialidad, privacidad que son riesgos que el responsable debe saber cómo afrontar. La adopción de tecnologías debe considerar, por un lado, la regulación interna que acompaña al sector público y, además, los asuntos de privacidad

44 Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679 (WP 248/2017).

45 https://www.govinfo.gov/content/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf

y confidencialidad en el tratamiento de los datos y la responsabilidad por los actos de aquel que decide la automatización de ciertos procesos.

La propuesta de un sistema de responsabilidad es que la protección de los datos en la decisión automatizada no puede basarse en la ficción del consentimiento, sino en soluciones proactivas de responsabilidad, tales como la rendición de cuentas, transparencia, impugnación y las garantías exigibles que deben ser efectivamente supervisadas.

El asunto es que no todos los países cuentan con autoridades de control de datos que cumplan esta labor, quedando entonces estos criterios a la autorregulación del que trata los datos y a un riesgo aún mayor que asume el que, dentro de su negocio, si decide soslayar estos criterios.

Sin embargo, a pesar de la falta de un ente supervisor, es un fin último del Estado garantizar el bien común y, por lo tanto, debe impulsar la creación de infraestructuras tecnológicas que protejan a las personas y no que vulneren o sacrifiquen sus derechos en beneficio de otros objetivos. Asimismo, se debe impulsar a generar un entorno que estimule a la comunidad de investigación y al sector privado a dar esas soluciones tecnológicas, exigiendo a quienes contribuyen un nivel máximo de cuidado y estableciendo limitantes que permitan conciliar la técnica con los derechos de las personas.

Es por eso que insistimos que las autoridades de datos que pueden contribuir a generar este ecosistema y, que lejos de ser un obstáculo a la innovación, son todo lo contrario, pues entregan reglas claras y permiten disminuir los riesgos que afronta, cada vez, quien desea implementar estos sistemas, lo que finalmente incentiva un mayor desarrollo tecnológico.

Los países desarrollados se encuentran en una continua revisión y adopción de tecnologías como las descritas que permitan afrontar la cada vez más creciente demandas ciudadanas. La adopción de sistemas TIC, en el Estado, soluciona una enorme cantidad de problemas que van desde las inequidades de acceso, los tiempos de espera, la falta de personal idóneo y los problemas de la burocracia. Toda implementación de tecnología no solo debe apuntar hacia las mejores políticas públicas por las capacidades de analizar más datos más eficientemente, sino que en el centro están las personas. Por eso, su adopción debe considerar, por un lado, la regulación sobre todo los riesgos respecto de los asuntos de privacidad y confidencialidad en el tratamiento de los datos y la responsabilidad del que implementa una solución, por lo que significa la automatización de ciertos procesos.

La privacidad es solo uno de los riesgos a abordar; otro es la posible discriminación algorítmica, esto es un trato diferente y perjudicial que se da a una persona debido a categorizaciones arbitrarias o irrelevantes. Se la califica de "algorítmica" porque permite que la discriminación se instale y prolifere en los sistemas informáticos[46].

Justamente, la protección de datos como parte de un sistema desde su diseño puede mitigar este riesgo, bajo un proceso adecuado de recolección, almacenamiento, tratamiento de los distintos datos que luego serán reproducidos en el sistema de decisión.

46 Buenadicha, C., Galdon, G., Hermosilla, M. P., Loewe, D., & Pombo, C. (2019). La gestión ética de los datos.

La forma de entender el Derecho ha cambiado sustancialmente a lo largo del tiempo. La evolución de esta disciplina ha sido paulatina e influenciada por diversas fuentes, originadas en distintos momentos y latitudes.

La tecnología, por su parte, ha irrumpido en la vida humana de manera súbita, llegando a ser indispensable en nuestro día a día. Actualmente, se reconoce el impacto disruptivo que ha tenido en la manera de relacionarnos, de entender el mundo y nuestra propia sociedad. Tan es así que, en esa incesante carrera por llegar a todos los ámbitos de la vida y del conocimiento, la tecnología se encuentra, cara a cara, con el Derecho.

El reconocimiento del impacto que la tecnología está generando en el Derecho y en el ejercicio de la profesión es lo que da lugar al libro que tiene hoy entre sus manos, que es, además, el primero de su tipo publicado en el Perú. La presente obra colectiva está compuesta por veintinueve artículos escritos por profesores, académicos y abogados de distintos países, que abordan, entre otros temas, cómo es que el derecho se ve influenciado, tanto positiva como negativamente, por la tecnología, cómo es que ambos deberían relacionarse, y cuál es el futuro que este encuentro depara.

"The law is silver, but the knowledge is gold"

ISBN: 978-612-48087-0-8