

DOCTRINA

La Autoridad Nacional de Protección de Datos bajo la perspectiva del análisis costo-beneficio

*The National Data Protection Authority under
the view of the cost-benefit analysis*

Helimara Moreira Lamounier Heringer 

Universidade do Estado de Minas Gerais, Brasil

RESUMEN Este artículo trata sobre la institución de una Autoridad Nacional de Protección de Datos, desde la perspectiva de la aplicación de los conceptos de análisis de impacto normativo y la herramienta análisis costo-beneficio. Bajo la aplicación de estas herramientas como instrumentos mitigadores de influencias no deseadas en la toma de decisiones regulatorias, se analiza la posibilidad o no de una autoridad nacional que pueda desligarse de influencias políticas y económicas de sectores específicos de la sociedad, con la creación de políticas de protección que acompañen el creciente desarrollo tecnológico del entorno virtual.

PALABRAS CLAVE Protección de datos personales, Ley General de Protección de Datos Personales, autoridad nacional, análisis de impacto regulatorio, análisis costo-beneficio.

ABSTRACT This article deals with the institution of a National Data Protection Authority from the perspective of applying the concepts of regulatory impact analysis and the cost-benefit analysis tool. Under the application of these tools as mitigating instruments of unwanted influences in regulatory decision-making, it analyzes the possibility or not of a national authority that is as disconnected as possible from political and economic influences of specific sectors of society, with the creation of policies of protection that accompany the growing technological development of the virtual environment.

KEYWORDS Data protection, General Data Protection Law, national authority, regulatory impact analysis, cost-benefit analysis.

Introducción

La protección de datos personales es uno de los temas más sensibles derivados de la revolución tecnológica de Internet. La garantía de los derechos individuales y colectivos relacionados con el secreto y la privacidad ha demandado un gran esfuerzo en el sentido de crear mecanismos que permitan la protección y eviten la difusión no autorizada de datos personales y la exposición de datos sensibles o no personales.

En 2016, en plena campaña electoral para la Presidencia de Estados Unidos, el sitio web Wikileaks publicó un archivo que contiene más de 30.000 correos electrónicos y archivos adjuntos de la entonces candidata Hillary Clinton, recibidos y enviados desde su correo electrónico personal mientras era secretaria de Estado en la administración Obama.¹ En 2019, en Brasil, la revista electrónica *The Intercept* (Brasil) publicó varias conversaciones personales realizadas a través de aplicaciones móviles por los integrantes de la denominada «Operación Lava-jato»,² obtenidas mediante interceptaciones de *hackers*, en el episodio conocido como «Vaza-jato». También en 2019, los datos personales de 540 millones de usuarios de Facebook estuvieron expuestos en los servidores de Amazon.³ Sin entrar en los méritos de los contenidos allí expuestos y la rendición de cuentas, en cada caso, lo que se evidencia es la fragilidad relacionada con la protección de datos personales que aún existe en el entorno virtual.

La creciente preocupación de gobiernos, empresas y entidades relacionadas con el tema, respecto al control y seguridad de esta información, ha llevado en todo el mundo a la formulación de políticas y normas que tienen como objetivo promover mecanismos y estrategias que permitan garantizar la seguridad y privacidad del ciudadano titular de los datos personales.

Entre estos mecanismos, la creación en casi todos los países de la llamada autoridad nacional de protección de datos personales, que en Brasil se conoce con el acrónimo ANPD, es una de las principales apuestas en el objetivo de proteger esta información sensible para la privacidad de las personas. La regulación del sector es una de sus principales funciones.

Este trabajo busca estudiar la pertinencia y viabilidad de una autoridad nacional desconectada de las influencias políticas y económicas de sectores específicos de la sociedad, presentando el método de análisis de impacto regulatorio (AIR) y la herramienta de análisis costo-beneficio (ACB), en particular, como instrumento capaz de mitigar las influencias no deseadas en la toma de decisiones regulatorias y permitir la producción de normas idóneas para la creciente demanda de nuevas tecnologías que pueden poner en peligro la privacidad y los datos personales de los ciudadanos.

1. Tom Hamburger y Karen Tumulty, «WikiLeaks releases thousands of documents about Clinton and internal deliberations», *The Washington Post*, 22 de julio de 2016. Disponible en <https://bit.ly/3NPWXID>.

2. Glenn Greenwald, Betsy Reed y Leandro Demori, «As mensagens secretas da Lava Jato», *Intercept Brasil*, 9 de junio de 2019. Disponible en <https://bit.ly/3PXRmmf>.

3. Portal G1, «540 milhões de dados de usuários do Facebook ficam expostos em servidores da Amazon», *Grupo Globo*, 4 de abril de 2019. Disponible en <https://bit.ly/3rv4GVe>.

Dichos análisis se realizarán a través de la investigación doctrinal y en función de la legislación pertinente.

El desafío de la protección de datos personales

Hasta principios del siglo XX, la cantidad de información que producía la sociedad estaba limitada de forma directamente proporcional a las dificultades existentes para su difusión. Respecto a los datos personales, el individuo poseía un número básico de información, que se limitaba a una fecha de nacimiento, documentos de registro y preferencias básicas. Con el desarrollo tecnológico, especialmente en el campo de la comunicación, el volumen de información producido creció exponencialmente, ampliando la gama de información personal circulante, que puede ir desde contraseñas hasta movimientos físicos registrados por el sistema de posicionamiento global del vehículo o teléfono celular (GPS), por ejemplo, transformando estos datos en un valioso activo de mercado, que requiere la debida protección en el ámbito práctico y legal. Como señala Danilo Doneda:

Las bases de datos que contienen datos personales, tan comunes en la actualidad, brindan una nueva definición de poderes y derechos sobre la información personal y, en consecuencia, sobre la persona misma. Aumenta el número de sujetos que pueden tener acceso a un conjunto cada vez más detallado y preciso de información sobre terceros, lo que hace que el estatuto jurídico de estos datos se convierta en uno de los puntos centrales que definirán la propia autonomía, identidad y libertad del ciudadano contemporáneo (2011: 93).⁴

Esta reconfiguración de poderes es la razón por la cual el debate sobre el tema de la protección de datos personales es urgente. La fragilidad del individuo frente a la capacidad de alcanzar, invadir y dominar a los controladores de su privacidad rediseña la forma de relacionarse, social y políticamente, y amenaza uno de los pilares de la democracia: la libertad individual.

El desarrollo histórico de la protección de datos en Brasil

La sociedad actual está configurada en forma de redes de información; estructuras físicas construidas a partir de sistemas satelitales y redes de fibra óptica conectan al mundo en una relación de interdependencia global, en la que fronteras y mercados se funden en un mismo fenómeno: la globalización. El concepto de *cibernética*, común a los laboratorios y centros tecnológicos y militares desde la Segunda Guerra Mundial, llegó a los hogares y utensilios domésticos a través de la red informática mundial o *world wide web* (triple «w»).

Todos los agentes, públicos y privados, demandan información veraz de forma cada vez más rápida. La informática es la técnica que responde a este anhelo social, trayen-

4. Traducción libre de la autora.

do agilidad, oportunidad y confiabilidad a la circulación de la información. En la hoy denominada «sociedad de la información», la riqueza económica y la concentración del poder ya no se basan en viejos paradigmas clásicos, como la propiedad de la tierra o de los medios de producción; la riqueza actualmente se traduce en el acceso que se tiene —sea un Estado, una corporación u otros— a las fuentes de materias primas y de trabajo, a las tecnologías de producción y, especialmente, al mercado de consumo, es decir, a la información misma (Castro, 2002: 41).

A cada instante, miles de piezas de información son generadas y procesadas virtualmente en el entorno web, en los más diversos sectores de la sociedad, tanto públicos como privados. En el ámbito personal, diariamente se generan, recopilan y procesan elementos como el ADN, huellas dactilares, datos médicos, preferencias de consumo y antecedentes proporcionados por el individuo en redes sociales, entre otros, que contienen información significativa que permite mapear demandas de mercado, tendencias de consumo, preferencias políticas y opiniones susceptibles de interferir y determinar la toma de decisiones económicas, en la esfera privada, y políticas y sociales, en el público (Borges, 2019). En palabras de Danilo Doneda:

La preocupación creciente con respecto a la protección de la privacidad es típica de nuestro tiempo. Pero la idea de privacidad en sí no es reciente. Con los diferentes significados que presenta, se puede identificar en otras épocas y en otras sociedades. Sin embargo, con sus características actuales, comenzó a ser notada por el sistema legal a fines del siglo XIX y adquirió sus características actuales solo en las últimas décadas. Ciertamente, no había lugar para la protección legal de la privacidad en sociedades que confiaban su regulación a otros mecanismos, ya sea una jerarquía social rígida o bien la arquitectura de los espacios públicos y privados; ya sea porque las pretensiones al respecto fueron neutralizadas por un ordenamiento jurídico corporativo o patrimonialista; o bien fue porque, en sociedades para las que la privacidad no representaba más que un sentimiento subjetivo, no merecía protección (2006: 92).⁵

La excesiva producción y tratamiento de datos personales reaviva el debate sobre la privacidad como derecho individual, en el que existe una importante contradicción. Por un lado, la protección de la intimidad de las personas y el derecho a la libertad se refleja en varios documentos internacionales, como ocurre con la Carta de los Derechos Fundamentales de la Unión Europea, en la que se reconoce la protección de datos como un derecho fundamental autónomo (Rodotà, 2009). Por otra parte, temas como la seguridad nacional, la protección contra el terrorismo y el control social, en el ámbito público, y los intereses del mercado, en el mundo privado, han llevado cada vez más a gobiernos y empresas a traspasar los límites de las salvaguardias y garantías esenciales del derecho a la intimidad y protección de datos. Poco a poco, la privacidad está saliendo del ámbito de los derechos fundamentales y, a menudo, se considera un obstáculo para la seguridad colectiva.

5. Traducción libre de la autora.

La informatización de los datos permite el almacenamiento detallado de la información personal de las personas. Esta abundancia de antecedentes expone la vulnerabilidad de los datos personales, especialmente de aquellos considerados sensibles por la legislación vigente.

Al respecto, John Barlow señala que:

Los datos personales de los consumidores siempre han sido atractivos para el mercado. Con datos precisos sobre los consumidores, es posible, por ejemplo, organizar una planificación más eficiente de productos y ventas, o incluso publicidad enfocada en las características reales de los consumidores, entre muchas otras posibilidades. No hace mucho tiempo, el costo de obtener dichos datos personales solía restringir severamente la cantidad de esta información que realmente se recopilaba y usaba (2010: 9).⁶

En Brasil, el marco normativo sobre protección de datos y privacidad se encuentra en la Constitución Federal, que tiene como una de sus garantías individuales la inviolabilidad de la intimidad y la vida privada, la correspondencia y los datos telegráficos, y las comunicaciones telefónicas; en la Ley de Habeas Data (Ley 9.507 de 1997), que regula el derecho de acceso a la información en poder del Estado; en el Código de Defensa del Consumidor, que garantiza a las personas no solo poder acceder a sus datos personales contenidos en registros y archivos, sino también a un debido tratamiento de esta información; en la Ley Positiva de Registro (Ley 12.414 de 2011), que resguarda la formación y consulta de bases de datos con información e historial crediticio de personas naturales o jurídicas; en la Ley de Acceso a la Información (Ley 12.527 de 2011), que define el concepto de información personal como aquella relacionada con una persona identificada o identificable; y en el Marco de Derechos Civiles en Internet (Ley 12.965 de 2014), que no obstante delimitar responsabilidades en el entorno web, no logró garantizar la privacidad y protección de datos de manera integral, completa y estructurada.

Esta última, en particular, abordó la responsabilidad civil que correspondería a los proveedores de Internet ante eventuales daños al honor, la imagen, vida privada o intimidad de las personas, y presentó normas innovadoras para la protección de datos personales, tales como el control de prácticas abusivas, garantías de confidencialidad de las comunicaciones y prohibición de llevar registros de acceso a los servicios de Internet.

Sin embargo, uno de los aspectos relevantes que caracterizan al Marco de Derechos Civiles de Internet es su incapacidad para innovar y disciplinar el entorno virtual de la web, así como de ofrecer una estandarización que regule el sector, puesto que, básicamente, repite la legislación existente en ese momento, sin agregar nuevas características. Este es el caso del artículo 7 número 13 de la misma, que establece la aplicación de normas de protección y defensa del consumidor únicamente en las relaciones comerciales realizadas en Internet.

6. Traducción libre de la autora.

Es así como de esta necesidad de actualización, en 2018 surge la Ley 13.709, modificada un año más tarde por medio de la Ley 13.853, que, entre otros cambios, le da su nombre actual: Ley General de Protección de Datos Personales, nuevo ordenamiento jurídico que ha demostrado ser relevante y capaz de promover un avance normativo en materia de protección de datos y derecho a la privacidad.

La Ley General de Protección de Datos Personales

En términos generales, la Ley 13.709 se refiere al tratamiento que se le da a cualquier tipo de registro personal o base de datos, física o electrónica, que tenga una empresa o entidad, pública o privada, y cómo debe ser tratada esta información, en cuanto a su recolección, producción, recepción, clasificación, uso, acceso, reproducción, transmisión, distribución, procesamiento, archivo, almacenamiento, eliminación, evaluación o control, modificación, comunicación, transferencia, difusión o extracción.

Aprobada en agosto de 2018, esta ley estuvo fuertemente influenciada por el Reglamento General de Protección de Datos, aprobado por la Unión Europea en mayo del mismo año, y cuyo objetivo, además de resguardar los datos de personas físicamente ubicadas en el ámbito de acción del bloque, es proteger tanto el flujo de datos existente entre los países miembros como las transferencias que se desarrollen en o con destinos fuera de sus fronteras, pero que conciernen a ciudadanos europeos.

La Ley General de Protección de Datos Personales, por su parte, regula cómo serán tratados los datos personales en el país y en el exterior, pero solo si esta información ha sido extraída o el interesado se encuentra en Brasil. Además, determina que los sectores público y privado deben alinearse con prácticas de recolección, uso, procesamiento, almacenamiento y difusión de los datos personales de sus clientes externos (consumidores) e internos (empleados y colaboradores). Con base en la normativa europea, las empresas, entidades y organismos privados, así como municipios y empresas públicas, deben mapear el flujo de estos datos personales, actualizando sus políticas de seguridad y privacidad, con el fin de garantizar el secreto y privacidad de sus clientes y usuarios.

En cuanto a la conceptualización de los datos personales, la ley brasileña, al igual que su par en Europa, adoptó el concepto expansionista en detrimento del reduccionista.⁷ Es decir, desde un punto de vista conceptual más amplio, considera como personal cualquier dato que se relacione directamente con una persona determinada o que pue-

7. La orientación reduccionista se basa en una lógica restrictiva según la cual los datos personales son información que debe asociarse a una persona específica. Debe ser un signo que permita establecer un vínculo inmediato o directo con su titular, individualizándolo con precisión. Los datos para ser personales deben, por tanto, ser la proyección de una persona única e inequívoca (identificada). El concepto expansionista, al contrario, apuesta por una lógica más flexible, que prescinde de la asociación exacta entre un dato y una persona. Los datos personales pueden ser cualquier tipo de información que permita la identificación de un individuo, incluso si el vínculo no se establece de manera inmediata y de forma directa. En este caso, entonces, los datos para ser personales deben, por tanto, ser la proyección de una persona identificable (Bioni, 2015: 17).

da ser identificable, lo que hace que sea más restrictiva, al abarcar una gama más amplia de datos vistos como personales.

Desde el punto de vista de la protección y garantía de la privacidad, uno de sus principales elementos es la prohibición que tienen empresas e instituciones de transmitir dichos datos sin el consentimiento del interesado; salvo en casos específicos previstos en la ley, como ocurre con una orden judicial (artículos 7 y 8).

Otra característica a destacar es la adopción del concepto de anonimización de los datos para su difusión y distribución, proceso mediante el cual se manipula la información de una base para dificultar la identificación de los interesados: «El anonimato juega un papel central en el manejo moderno de datos, formando el núcleo del procedimiento estándar para almacenar o divulgar información personal» (Ohm, 2010: 1707). El autor destaca que, si bien un responsable del tratamiento de datos personales puede almacenarlos en una base física o electrónica de forma identificable, manteniendo la privacidad de los titulares de los datos, también puede conservar otros registros que contengan los mismos datos utilizando la anonimización o seudonimización de los mismos.

Si bien existen muchas técnicas de anonimización diferentes, con costos y niveles de confiabilidad igualmente variables, ninguna de ellas está exenta de someterse al proceso inverso, esto es, de reidentificación o desanonimización; lo que hace que la búsqueda de la privacidad no sea solo una cuestión jurídica de garantía de derechos, sino un desafío tecnológico.

La ley de protección de datos brasileña, en consonancia con las principales normativas del tipo a nivel mundial, se apoya en los siguientes fundamentos: a) respeto a la privacidad y autodeterminación informativa; b) libertad de expresión, información, comunicación y opinión; c) inviolabilidad de la intimidad, el honor y la imagen; d) desarrollo económico, tecnológico e innovación; e) libre iniciativa, libre competencia y protección al consumidor; y f) protección a los derechos humanos, el libre desarrollo de la personalidad, la dignidad y el ejercicio de la ciudadanía por parte de las personas naturales.

Además, la ley se guía por una serie de objetivos,⁸ tales como garantizar el derecho de decisión del titular sobre el destino y uso de los datos; el establecimiento de medi-

8. En ese sentido, la Ley General de Protección de Datos Personales estableció los siguientes principios: a) finalidad, que existen fines legítimos, determinados, explícitos e informados al titular para el tratamiento de los datos personales; b) idoneidad, que el tratamiento de los datos sea compatible con la finalidad; c) necesidad, limitación del tratamiento al mínimo necesario para el cumplimiento de sus finalidades; d) libre acceso, garantía, a los titulares, del conocimiento sobre la forma y duración del tratamiento de sus datos personales; e) calidad de los datos, garantía a los titulares de la exactitud, claridad, pertinencia y actualización de los datos; f) transparencia, acceso garantizado al tratamiento y a los respectivos agentes a cargo de este, y salvaguarda de los secretos comerciales e industriales; g) seguridad, protección de los datos personales tratados; h) prevención, adopción de medidas para evitar la ocurrencia de daños con motivo del tratamiento de datos personales; i) no discriminación, prohibiendo el tratamiento para fines discriminatorios ilícitos o abusivos; y j) rendición de cuentas, la observancia y el cumplimiento de las normas de protección de datos personales, so pena de responsabilidad punitiva.

das que prevengan o minimicen los daños causados por el mal uso de la información personal; limitar el uso de datos personales por parte de terceros a lo estrictamente necesario; el derecho del titular a la integridad, exactitud, acceso y corrección de los datos personales; y la responsabilidad de cada cual en caso de incumplimiento de estos preceptos generales.

La ley también clasifica los datos personales en dos niveles bien diferenciados: generales y sensibles; siendo estos últimos aquellos relacionados con el origen racial o étnico de la persona, credo, opiniones políticas, afiliación sindical o a organizaciones de carácter religioso, filosófico o político, salud, vida sexual, información biométrica, etcétera. Otros datos que puedan estar relacionados con una persona determinada o identificable son de carácter general.

Cabe destacar que, velando por un «interés superior», la normativa restringe el uso de datos personales —generales o sensibles— de niños, niñas y adolescentes, y su tratamiento debe realizarse contando con el consentimiento específico y destacado de, al menos, uno de los padres o tutores legales.

Además, la ley establece los derechos de los titulares, los criterios para el uso y tratamiento de los datos personales, los agentes que podrán utilizarlos, las sanciones por el incumplimiento de sus disposiciones y, previa aprobación de la Ley 13.853 de 2019, la creación de la Autoridad Nacional de Protección de Datos.

Sobre esto último, un aspecto significativo de la nueva legislación fue el posterior veto que se hizo de los artículos que crearon tanto la Autoridad Nacional como el Consejo Nacional de Protección de Datos (artículos 55 a 59 de la Ley 13.709), siendo la ley sancionada sin el establecimiento de un organismo regulador y supervisor de las determinaciones contenidas en sus disposiciones, cuestión que será tratada en el siguiente apartado.

La institución de la Autoridad Nacional de Protección de Datos

Es indispensable la existencia de una autoridad nacional encargada de la tutela y protección de la información de las personas en el ámbito digital; es un organismo garante y actor principal en la promoción de políticas públicas y regulación relacionada con la privacidad y el tratamiento de datos personales (Borges, 2019: 177-272).

La tendencia en las leyes contemporáneas de protección de datos (etiquetadas como de cuarta generación) es suponer que el resguardo de esta información no debe dejarse a la mera elección individual. Admitiendo la existencia de un fuerte desequilibrio en la relación entre el interesado y los encargados del tratamiento, que no se nivela con el simple reconocimiento del derecho a la autodeterminación informativa, estas leyes, paradójicamente, buscan reducir el control de las personas y elevar la función de una autoridad capaz de garantizar los derechos individuales, instalando instrumentos jurídicos en la esfera colectiva de protección, con el fin de fortalecer la posición del individuo frente a las entidades que manejan sus datos (Doneda, 2011: 91-108).

Recurrir a una autoridad nacional independiente para la regulación de la protección de datos personales es una tendencia adoptada en varios países. Su papel en la aplicación eficiente de las leyes de protección de datos permite una protección eficaz de la privacidad de los ciudadanos al tiempo que proporciona seguridad jurídica en la interpretación y aplicación de la ley, algo bastante evidente al analizar la experiencia de los países que adoptaron el modelo (Borges, 2019: 190).⁹

En el otro extremo se encuentran las empresas e instituciones que poseen y operan innumerables bases de datos personales. Para estos actores es vital una comprensión total del papel que desempeñan las autoridades nacionales de protección de datos; sobre todo, porque estas entidades públicas, por regla general, no solo tienen poderes regulatorios, sino también ejecutivos y de supervisión, contando con la capacidad de imponer multas sustanciales e interferir con su autonomía de acceso a estas bases de datos.

Independientemente del tipo de negocio que lleve a cabo la organización, ya sea privada o pública, las autoridades nacionales tienen potestad para hacer cumplir las leyes de protección de datos y regular las actividades comerciales e institucionales relacionadas con el procesamiento de información personal.

Desde esta perspectiva, una entidad pública creada para estos fines específicos en Brasil ha debido transitar un camino bastante truncado y viene con un retraso considerable respecto a otros países del mundo.

Cuando fue sancionada, en agosto de 2018, el veto en la ley de los artículos que establecían la Autoridad Nacional y el Consejo Nacional de Protección de Datos se justificó únicamente en que «los dispositivos incurren en inconstitucionalidad del proceso legislativo, como una afrenta al artículo 61, párrafo 1, II, letra e), combinado con el artículo 37, XIX, de la Constitución»,¹⁰ enfatizando en la competencia exclusiva del Poder Ejecutivo para la creación de tales órganos de la administración pública; sin que esto signifique, por supuesto, que no se puedan promover los medios para la creación posterior de una autoridad nacional y del consejo.

Para llenar este vacío, en diciembre de 2018, el gobierno emitió la Medida Provisional 869, que en julio de 2019 el Congreso Nacional se encargó de aprobar y transformar en la Ley 13.853, y que, entre otras consideraciones, fija incluir en el artículo 55 de la Ley 13.709 la creación tanto de un consejo como de una autoridad nacional, con énfasis en el artículo 55-B, que garantiza la autonomía de decisión de esta última.

A pesar de todas las controversias en torno a la aprobación de la medida provisional del Ejecutivo, y que se tratarán más adelante, Brasil cuenta hoy con una Ley General de Protección de Datos Personales, con derecho a establecer una autoridad nacional a cargo del tema; eso sí, con cerca de cincuenta años de atraso respecto de la principal legislación en la materia.

9. Traducción libre de la autora.

10. Secretaría General de la Presidencia (Brasil). Mensaje 451, del 14 de agosto de 2018, mediante el cual se vetan parcialmente disposiciones del PL 53, que da origen a la Ley 13.709, de Protección de Datos Personales. Disponible en <https://bit.ly/44otigQ>.

La composición de la Autoridad Nacional de Protección de Datos Personales

Esta autoridad, como se mencionó, prevista en la ley original y vetada durante la administración del presidente Michel Temer, estaría vinculada al Ministerio de Justicia, con «carácter de una autarquía especial [...] y caracterizada por la independencia administrativa, ausencia de subordinación jerárquica, mandato fijo y estabilidad de sus líderes y autonomía financiera».¹¹

En el texto final, añadido por el artículo 55-A, párrafo 1, de la Ley 13.853 de 2019, la naturaleza jurídica de la Autoridad Nacional de Protección de Datos es transitoria, pudiendo ser transformada por el Poder Ejecutivo en un órgano de la administración pública federal indirecta, y vinculado a la Presidencia de la República.

La entidad está integrada por una Junta Directiva, máximo órgano de gobierno; el Consejo Nacional de Protección de Datos Personales y Privacidad; un departamento de Asuntos Internos; un Defensor del Pueblo; su propio cuerpo de asesoría legal; y por las unidades administrativas y especializadas necesarias para la aplicación de las disposiciones de la ley.

La autoridad cuenta con atribuciones que le otorgan el rol de guardián de los datos personales en el país, con funciones administrativas, normativas, resolutivas, rectoras, de supervisión y sancionadoras. Entre las 24 competencias propias de este organismo, destacan el celo por la protección de datos personales, en los términos contenidos en la legislación; la elaboración de lineamientos para una política nacional de protección de datos personales y privacidad; la emisión de normas y procedimientos sobre protección de antecedentes y privacidad; y la supervisión y exclusividad en la aplicación de sanciones en caso de que el tratamiento de datos realizado infrinja la ley.

En el proceso legislativo que culminó con la aprobación y sanción de la Ley 13.853, el legislador realizó importantes adiciones a la Medida Provisional 869 de gobierno, siendo la autonomía técnica y de decisión de la Autoridad Nacional de Protección de Datos la más significativa de ellas. En el texto original, solo se preveía la autonomía técnica, sin otorgar soberanía a la toma de decisiones del nuevo organismo. Esta enmienda representa un paso hacia su independencia. Sin embargo, la administración del presidente Temer impuso vetos sobre el cobro de honorarios y servicios prestados, cuestiones que limitan el presupuesto de la agencia y la hacen financieramente dependiente del Poder Ejecutivo, amenazando con ello su independencia y autonomía, que quedan a merced de eventuales influencias que puedan ejercer grupos políticos o gobiernos de turno.

La cuestión de la autonomía de la Autoridad Nacional de Protección de Datos

A diferencia de los organismos reguladores, que son entidades de la administración pública indirecta, es decir, una autarquía bajo régimen especial, la nueva autoridad fue

11. Secretaría General de la Presidencia (Brasil). Mensaje 451, del 14 de agosto de 2018, mencionado en la nota 10. Disponible en <https://bit.ly/44otigQ>.

creada como un órgano de la administración pública directa, esto es, inmediatamente vinculada a la Presidencia de la República. Si bien esta naturaleza jurídica es transitoria, según lo previsto en el párrafo 1 del artículo 55-A de la Ley General de Protección de Datos Personales, y puede transformarse en una autarquía de la administración pública indirecta, el mismo párrafo dispone que esta gobernanza autónoma quedará ligada a la Presidencia de la República.

Aunque la función ejecutiva de los organismos reguladores, competencia que implica actos de autoadministración, regulación, inspección y sanción, se basa en la implementación de políticas públicas y lineamientos establecidos por el legislador (Barroso, 2002: 301-302), asimismo se les garantiza la inexistencia de un vínculo jerárquico o decisorio con la administración pública directa, siendo estas agencias la última instancia administrativa para juzgar los recursos contra sus propios actos, lo que hace impropio el control administrativo vía recurso jerárquico e improcedente la revisión por parte de un agente público (ministro o secretario de Estado) de las decisiones tomadas por ellos. En este sentido, la simple comparación de su naturaleza jurídica es suficiente para permitir afirmar que los órganos reguladores tienen más autonomía que la autoridad encargada de la protección de datos.

Este es un tema delicado, ya que, si bien el artículo 55-B asegura la autonomía técnica y de decisión de la autoridad, por ser el ente encargado de salvaguardar un derecho constitucional, como es la protección de datos, su vinculación a la Presidencia de la República y dependencia presupuestaria pueden afectar significativamente sus niveles reales de autonomía, en razón de limitaciones operativas o de recursos que impidan su adecuado desarrollo y proyección.

No cabe duda de que la independencia de esta autoridad nacional es indispensable para la protección de los ciudadanos, la garantía del equilibrio en el flujo transnacional de datos y la defensa de la democracia. Sin embargo, ¿cómo se puede garantizar su exención del poder económico y político? ¿Cómo protegerla de estas influencias? Sin duda, este es el desafío «casi» sin gloria a abordar por el legislador y que debe ser salvaguardado por el Poder Judicial.

Autonomía de la Autoridad Nacional de Protección de Datos desde la perspectiva costo-beneficio

La Carta de los Derechos Fundamentales de la Unión Europea, en su artículo 8 número 3 establece que «el cumplimiento de estas normas [sobre la protección de datos personales] quedará sujeto al control de una autoridad independiente».¹² Desde las primeras normas, la existencia de una autoridad ha sido un sello distintivo de la legislación europea sobre protección de datos.

12. Carta de los Derechos Fundamentales de la Unión Europea (2000/C364/01). Disponible en <https://bit.ly/3pLqfAa>.

Respecto a su independencia, esta se justifica en un marco legal que le permita ser eficaz y siempre y cuando exista un enfoque estratégico capaz de marcar diferencias en la relación entre el titular y los responsables del tratamiento y operación de datos personales, requiriendo una actuación más eficaz por parte de los agentes de control, a fin de defender los valores y derechos relacionados con la privacidad (Hustinx, 2009: 131-137).

Otro aspecto relevante para determinar la eficacia de una autoridad de protección de datos es cuestionar y evaluar en qué medida tiene la habilidad y capacidad suficientes para mantenerse al día con el constante y creciente desarrollo tecnológico, para de esta forma producir y mantener normas suficientemente efectivas en la materia (Raab y Szekely, 2017: 421-433).

Al igual que con el *software* y equipos que utilizamos, el volumen de tecnologías que surgen constantemente para el manejo y procesamiento de datos, personales o no, puede hacer que una regulación quede obsoleta en cuestión de días. Y actualizar este reglamento y los propios comisionados de la Autoridad Nacional de Protección de Datos es un desafío importante.

Teniendo en consideración al menos estas dos cuestiones, esto es, la influencia político-económica y la dificultad de actualización debido al creciente volumen de tecnologías de procesamiento de datos, este trabajo parte por evaluar el papel de la autoridad desde una perspectiva de análisis costo-beneficio.

Estado regulatorio y análisis de impacto regulatorio

El desempeño económico de un país, por regla general, es evaluado a partir de parámetros como el producto interno bruto y la tasa de empleo, entre otros; elementos cuantitativos que permiten una medición constante y segura del desarrollo o no de una economía. Difícilmente se puede hacer un análisis similar sobre la efectividad de una regulación aplicada por un gobierno o una agencia reguladora, ya que no siempre es posible cuantificar los efectos o resultados esperados de una regla.

Desde un escenario económico en la década de 1980 que pedía menos Estado, la responsabilidad del liderazgo estratégico del crecimiento ha sufrido una transición hacia el sector privado (Sunstein, 2018). Este camino, en un primer momento, condujo a una severa liberalización del mercado, lo que trajo problemas derivados de la ausencia de salvaguardas de competencia efectiva y la posterior búsqueda de estructuras regulatorias para un crecimiento adecuado. La regulación marcó un retorno al equilibrio entre el papel del Estado y el mercado, y se convirtió en un instrumento fundamental para el desarrollo sostenible y la consolidación democrática. Es aquí cuando surge el Estado regulador, más limitado en su capacidad para utilizar herramientas de control macroeconómico, como son las políticas fiscal y monetaria, y más dependiente de su capacidad fiscalizadora (Ladegaard, 2005).

Es en este contexto de un Estado cada vez más propenso a la regulación que surgen legítimas dudas, muchas veces sin respuesta, sobre la real eficacia y conveniencia de las normas que ordenan a los distintos sectores de la sociedad. Las regulaciones, a menudo

creadas para responder a presiones políticas y/o económicas de ciertos sectores y coyunturas específicas, no se analizan en términos de los beneficios y costos aparejados para la sociedad en su conjunto.

El análisis de impacto regulatorio es el instrumento utilizado por la mayoría de los países desarrollados para comprender el efecto de las leyes en ámbitos relacionados con lo económico, social o ambiental, en un escenario donde se exige cada vez más a los gestores legislativos el poseer la capacidad de verificar el aporte de cualquier iniciativa al entorno del mercado y la sociedad en general.

Al ser este análisis visto como una herramienta para la toma de decisiones, puede ser utilizado con diferentes enfoques —de acuerdo con la agenda política de cada gobierno— y aplicarse a materias relacionadas con la evaluación de impacto ambiental, temas económicos, o incluso en términos de cargas administrativas y burocráticas, incluyendo (de ser requerido) una evaluación completa de costo-beneficio, examinando de manera consistente y sistemática los posibles impactos resultantes de la regulación y brindando información relevante a los tomadores de decisiones (Jacobs, 1997: 13-30).

En suma, este análisis permite verificar la necesidad o no de regulación y las implicaciones de su implementación, a fin de maximizar los beneficios netos para la sociedad.

Esencialmente, el AIR es un tipo de procedimiento administrativo, a menudo utilizado en el escrutinio prelegislativo. Su sofisticación y amplitud analítica varían, dependiendo de los temas en juego y los recursos disponibles; el grado de sofisticación debe ser proporcional a la relevancia y los efectos esperados de la regulación. De hecho, el análisis de los efectos esperados a través de AIR puede cubrir cargas administrativas o costos básicos de cumplimiento, o tipos más complejos de costos y beneficios, incluidos los beneficios ambientales, los efectos de distribución y el impacto en el comercio (Radaelli y De Francesco, 2010: 2).¹³

El análisis de impacto regulatorio debe ser continuo o sistemático, sin dejar lugar al oportunismo o posibles intereses de grupos políticos o económicos. Es obligatorio en los países donde se ha implementado y su evaluación no entra en el ámbito discrecional de la administración pública. Si bien es un instrumento que genera beneficios para la mejora de la calidad regulatoria, es un procedimiento complejo y extenso, que exige:

Apoyo político de niveles jerárquicos superiores, el establecimiento de un órgano central que promueva su uso, la integración del AIR en el proceso de desarrollo de políticas desde su concepción, una selección de metodologías flexibles y administrativamente viables, el desarrollo de estrategias de recopilación de datos precisos y confiables, la integración de mecanismos de consulta pública eficientes y el establecimiento de un programa intenso y continuado de formación de reguladores (De Sousa, 2012: 103).¹⁴

13. Traducción libre de la autora.

14. Traducción libre de la autora.

Las herramientas más utilizadas para evaluar los impactos de una acción regulatoria son los análisis costo-beneficio, costo-efectividad, multicriterio y de tipo parciales.

Análisis costo-beneficio y su aplicación a las autoridades y agentes reguladores

De todas las herramientas de evaluación regulatoria, el análisis costo-beneficio es reconocido como el que mejor se ajusta a este propósito (De Sousa, 2012: 102-103), ofreciendo la posibilidad de medir la efectividad de las regulaciones y analizar si son o no viables. Todo, como parte de un esfuerzo por superar decisiones basadas en intereses personales y políticos o evidencia anecdótica y suposiciones no científicas, a través de un enfoque fácilmente comprensible de las consecuencias reales de las iniciativas regulatorias y legislativas (Sunstein, 1996).

El análisis costo-beneficio refleja un firme (y orgulloso) compromiso con una concepción tecnocrática de la democracia. En última instancia, el público es soberano, pero por una buena razón: a los tecnócratas se les otorga mucha autoridad, que concede el mismo público [...]. El análisis costo-beneficio insiste en que las preguntas fácticas difíciles deben ser respondidas por aquellos que están en una buena posición para responderlas correctamente. La razón es que las consecuencias importan, y los científicos y economistas pueden ayudarnos a lidiar con las consecuencias (Sunstein 2018: 11).¹⁵

El análisis costo-beneficio de una regulación busca determinar si la utilidad generada (o el daño evitado) por esta es superior al esfuerzo y recursos involucrados en su desarrollo e implementación. En este esfuerzo, parámetros como muertes evitadas, enfermedades o daño ambiental, entre otros, se cuantifican en términos monetarios; aun cuando exista cierta dificultad para calcular muchos de los efectos en términos de salud y vida (Driesen, 2006: 1-71). Además, este análisis debe considerar una valorización de las capacidades y el costo de la tecnología utilizada para promover el resultado esperado, superen o no los costos y beneficios de no implementar una regulación en particular.

El consagrado análisis costo-beneficio, en su forma más simple, combinando sistemáticamente métricas cuantitativas y cualitativas, es la herramienta que mejor interpreta los intereses involucrados en la elaboración de una regla, ya que cubre una amplia gama de impactos en todo el espectro socioeconómico y ambiental, en línea con las demandas políticas casi universales que abarcan los métodos de análisis regulatorios (Jacobs, 1997: 13-30). A lo anterior se suma la importante ventaja que tiene de poder comparar costos y beneficios que ocurren en diferentes momentos.

Con esta técnica, los escenarios positivos y negativos más estrictos de las diversas opciones para resolver un problema se evalúan utilizando un enfoque que permite la comparación objetiva de las ventajas y desventajas de cualquier número de acciones alternativas utilizadas para resolver el problema.¹⁶

15. Traducción libre de la autora.

16. Comitê Brasileiro de Regulação (CBR). «The Brazilian Guide on Good Regulatory Practices» (2007). Disponible en <https://bit.ly/44JKJYV> (traducción libre de la autora).

Básicamente, no se puede emprender ninguna acción si el bien obtenido no compensa los gastos o recursos involucrados en su consecución; lo cual, en la práctica, sustrae las decisiones de regulación del campo político y del mero interés económico de sectores específicos, para adoptar una toma de decisiones basada en el conocimiento especializado y la búsqueda del equilibrio entre costo y beneficio (Sunstein, 2018).

Se puede argumentar que el análisis costo-beneficio, al menos si se practica de manera inteligente, puede proporcionar un contexto para hacer más transparentes las razones a favor y en contra de la regulación. Ciertamente, la técnica puede ayudar a distinguir los proyectos de obras públicas que valen la pena de los puentes que no conducen a ninguna parte (Sagoff, 2009: 25).¹⁷

Teniendo este método como pauta para la conducción regulatoria de la protección de datos personales, a través del trabajo de especialistas con capacidades técnicas necesarias, crece la posibilidad de que aquellas reglas provenientes de la autoridad nacional respondan a la pregunta sobre si sus beneficios compensan o no los costos en que se deba incurrir. Y puesto que entidad está ávida de responder a los criterios técnicos del análisis, se reduce la posibilidad de un desfase entre la norma y el desarrollo tecnológico del sector, además de mitigar la influencia que puedan ejercer sectores políticos, intereses económicos o, simplemente, la evidencia anecdótica e intuiciones no científicas.

Conclusión

La protección de datos personales es una de las garantías de un Estado democrático de derecho que consolida la condición de ciudadano de cada individuo. La fragilidad de los sistemas, el costo que genera el desarrollo de mecanismos de protección de antecedentes personales y la falta de normas que exijan esta garantía, debilitan el proceso democrático y transforman la información en una valiosa moneda de cambio e instrumento de poder, que ubica a los ciudadanos en una posición de desventaja frente a grandes corporaciones privadas y gobiernos que pueden ejercer un control excesivo sobre la sociedad.

La necesidad de mecanismos de protección y normativas que obliguen a los responsables del tratamiento a ser cuidadosos en el manejo de esta información, y que inhiban su manipulación con fines espurios, exigen contar con entes autónomos e independientes a cargo; demanda a la que diversos gobiernos han respondido con la creación de autoridades nacionales con competencias para regular, instruir, supervisar y sancionar eventuales faltas.

Sin embargo, y como ocurre a menudo, las decisiones de estas autoridades pueden estar sujetas a influencias de gobernantes, grupos políticos o intereses económicos, por lo que también se hace necesaria una regulación que limite su actividad a fines muy específicos y de interés general.

17. Traducción libre de la autora.

En el caso de la legislación brasileña, no existe disposición alguna que otorgue independencia a este organismo, así como tampoco que ordene una determinada formación y conocimiento del sector para sus funcionarios.

La composición de una Autoridad Nacional de Protección de Datos presupone la elección de un cuerpo técnico con autonomía y capacidad para tomar decisiones basadas en la ciencia mucho más que en la política.


Es por todo esto que la posibilidad de que un cuerpo técnico calificado utilice la herramienta de costo-beneficio para realizar un análisis de impacto regulatorio, se presenta como una excelente alternativa para satisfacer las dos demandas presentadas en el trabajo: la necesidad de una autoridad de protección de datos y la capacitación de sus componentes para desarrollar normas y mecanismos regulatorios acordes con el rápido y constante desarrollo tecnológico del entorno virtual de Internet.

Referencias

- BARLOW, John Perry (2010). «The new consumer is the product itself». En Danilo Doneda (elaboración), *A proteção de dados pessoais nas relações de consumo. Caderno de Investigação Científica 2*: 9-13. Brasília: Escola Nacional de Defesa do Consumidor. Departamento de Proteção e Defesa do Consumidor, Secretaria de Direito Econômico, Ministério da Justiça. Disponible en <https://bit.ly/3XNgePE>.
- BARROSO, Luis Roberto (2002). «Agências reguladoras: Constituição e transformações do Estado e legitimidade democrática». *Revista de Direito Administrativo*, 229: 285-311. DOI: [10.12660/rda.v229.2002.46445](https://doi.org/10.12660/rda.v229.2002.46445).
- BIONI, Bruno (2015). *Xeque-Mate: O tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil*. São Paulo: GPoPAI/USP. Disponible en <https://bit.ly/44Ccu5A>.
- BORGES, Maria Ruth (2019). «Autoridade Nacional de Proteção de Dados Pessoais: A importância do modelo institucional independente para a efetividade da lei». *Revista Caderno Virtual 2* (44): 177-272. Disponible en <https://bit.ly/3JUKxd>.
- CASTRO, Luis Fernando (2002). «Proteção de dados pessoais: Panorama internacional e brasileiro». *Revista CEJ*, 6 (19): 40-45.
- DE SOUSA, Renan Martins (2012). «A Análise de Impacto Regulatório (AIR) e o papel do Tribunal de Contas da União na avaliação da regulação setorial». *Revista do Tribunal de Contas da União*, 44 (123): 102-113. Disponible en <https://bit.ly/3PVurli>.
- DONEDA, Danilo (2006). *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar.
- . (2011). «A proteção dos dados pessoais como um direito fundamental». *Espaço Jurídico Journal of Law*, 12 (2): 91-108. Disponible en <https://bit.ly/3JRfgvZ>.
- DRIESEN, David (2006). «Is cost-benefit analysis neutral?». *The University of Colorado Law Review* (volumen 77). Disponible en <https://bit.ly/3N0mhyL>.

- HUSTINX, Peter (2009). «The role of Data Protection Authorities». En Serge Gutwirth, Yves Poullet, Paul de Hert, Cécile de Terwangne y Sjaak Nouwt (editoras), *Reinventing Data Protection?*, (pp. 131-137). Dordrecht: Spring Nature. DOI: [10.1007/978-1-4020-9498-9_7](https://doi.org/10.1007/978-1-4020-9498-9_7).
- JACOBS, Scott (1997). «Overview of regulatory impact analyses in OECD countries». En *regulatory impact analysis: Best practices in OECD countries* (pp. 13-30). París: OCDE. Disponible en <https://bit.ly/46FTDsl>.
- LADEGAARD, Peter (2005). «Improving business environments through regulatory impact analysis: Opportunities and challenges for developing countries». Artículo preparado para la Conferencia Internacional sobre la Reforma del Entorno Empresarial, El Cairo, Egipto. Disponible en <https://bit.ly/3pTWBsq>.
- OHM, Paul (2010). «Broken promises of privacy: Responding to the surprising failure of anonymization». *UCLA Law Review*, 57: 1701-1777. Disponible en <https://bit.ly/3NQ6ijR>.
- RAAB, Charles e Ivan Szekely (2017). «Data Protection Authorities and information technology». *Computer Law & Security Review*, 33: 421-433. DOI: [10.2139/ssrn.2994898](https://doi.org/10.2139/ssrn.2994898).
- RADAELLI, Claudio y Fabrizio De Francesco (2010). «Regulatory impact assessment». En Martin Cave, Robert Baldwin y Martin Lodge (editores), *The Oxford handbook of regulation* (pp. 279-301). Oxford: Oxford University. DOI: [10.1093/oxfordhb/9780199560219.003.0013](https://doi.org/10.1093/oxfordhb/9780199560219.003.0013).
- RODOTÀ, Stefano (2009). «Data protection as a fundamental right». En Serge Gutwirth, Yves Poullet, Paul de Hert, Cécile de Terwangne y Sjaak Nouwt (editoras), *Reinventing Data Protection?*, (pp. 77-82). Dordrecht: Spring Nature. DOI: [10.1007/978-1-4020-9498-9_3](https://doi.org/10.1007/978-1-4020-9498-9_3).
- SAGOFF, Mark (2009). «Regulatory review and cost-benefit analysis». *Philosophy & Public Policy Quarterly*, 29 (3/4): 21-26. DOI: [10.13021/G8pppq.292009.107](https://doi.org/10.13021/G8pppq.292009.107).
- SUNSTEIN, Cass R. (1996). «The cost benefit state». *Coase-Sandor Institute for Law & Economics Working Paper*, 39. *University of Chicago Law School*. Disponible en <https://bit.ly/3pLeiuq>.
- . (2018). *The cost-benefit revolution*. Cambridge: MIT.

Sobre la autora

HELMARA MOREIRA LAMOUNIER HERINGER es profesora de la Universidad del Estado de Minas Gerais (UEMG/Passos) y estudiante de doctorado y magíster en Derecho Colectivo y Ciudadanía, en la Universidad de Ribeirão Preto. Además, es becaria de la fundación CAPES, del Ministerio de Educación de Brasil. Su correo electrónico es helimarah@hotmail.com.  <https://orcid.org/0000-0002-3593-5223>.

REVISTA DE DERECHO PÚBLICO

La *Revista de Derecho Público* es publicada desde 1963 por el Departamento de Derecho Público de la Facultad de Derecho de la Universidad de Chile. Aparece dos veces al año. Su propósito es la difusión de los avances del derecho público nacional e internacional y la socialización de artículos de investigación inéditos de la comunidad académica nacional e internacional.

DIRECTORA

Ana María García Barzelatto

SECRETARIO DE REDACCIÓN

Felipe Peroti Díaz

fperoti@derecho.uchile.cl

SITIO WEB

revistaderechopublico.uchile.cl

CORREO ELECTRÓNICO

publico@derecho.uchile.cl

LICENCIA DE ESTE ARTÍCULO

Creative Commons Atribución Compartir Igual 4.0 Internacional



La edición de textos, el diseño editorial
y la conversión a formatos electrónicos de este artículo
estuvieron a cargo de Tipografía

www.tipografica.io