Licenciatura en Ciencia Política y Gobierno

Protección de Datos Personales en América Latina y el Caribe: un Estudio Comparado

Autoría: Herrero, Joaquín
Año de defensa de la tesis: 2023

UNIVERSIDAD TORCUATO DI TELLA

Departamento de Ciencia Política y Estudios Internacionales

Protección de Datos Personales en América Latina y el Caribe: un Estudio Comparado

Alumno: Joaquin Herrero

Tutor: Gastón Wright

Julio, 2023

Abstract

El presente estudio tiene como objeto realizar un análisis profundo de la protección de datos personales en América Latina y el Caribe. Hace foco en la dimensión *de iure* de la protección, tomando como unidades de análisis a las 19 leyes de protección de datos personales que han sido sancionadas hasta el momento en América Latina y el Caribe. Se tomó como horizonte normativo a la Regulación General de Datos Personales de la Unión Europea (GDPR, por sus siglas en inglés), a partir de la cual se formuló un marco metodológico compuesto por 160 variables y 7 índices.

Se construyó un Índice de Protección de Datos Personales de América Latina y el Caribe, el cual contempla numerosas dimensiones de la protección de datos, y compara con éxito 19 países de la región. El objetivo de la construcción de dicho índice es proponer un marco metodológico innovador para poder realizar evaluaciones continuas del estado de la protección de datos en la región desde la academia y la sociedad civil.

Se condujo un análisis de clúster, con el cual se brindó evidencia empírica robusta a favor de la existencia de grupos de leyes con características parecidas en la región. De esta forma, se aportó evidencia en favor de la primera hipótesis, la cual propone que *"no hay un marco regulatorio homogéneo respecto a la protección de datos personales en América Latina, sino que existen grupos de regulaciones de datos personales que cuentan con distintas características"*.

A su vez, se aportó evidencia muy sólida a favor de la hipótesis de que los países de la región de América Latina y el Caribe están emulando activamente el articulado de GDPR. Para este fin, se realizaron cuatro modelos de regresión lineal.

Introducción **2**
¿Por qué hablamos de datos personales? **3**
¿Cómo se protegen los datos personales? **7**
Derechos 8
Instrumentos 9
Consideraciones respecto del consentimiento 9
Transferencias internacionales 9
Responsable de tratamiento 10
Delegado de protección de datos (Data Protection Officer): 10
Autoridad de aplicación 10
Marco metodológico **12**
Índice de Consentimiento 14
Índice de Derechos 14
Índice de Instrumentos 15
Índice de Responsable de tratamiento 15
Índice de Delegado de protección de datos 15
Índice de Transferencias internacionales 15
Índice Autoridad de aplicación 16
La protección de datos personales en América Latina y el Caribe **17**
Datos como bien: facilitando un mercado 17
Datos como derecho, usuario como sujeto 18
Reafirmando el derecho del titular por sobre sus datos 20
La protección de datos conlleva medidas de seguridad y obligaciones: 21
Índice de Protección de Datos Personales de América Latina y el Caribe **23**
¿Cómo encontramos los grupos de leyes de protección de datos personales? **25**
¿Cuáles son los tipos de leyes de protección de datos personales en América Latina y el Caribe? **30**
Leyes con una baja protección de datos personales 30
Leyes con buena protección de derechos digitales 31
Leyes con autoridades robustas 32
Leyes abarcativas 32
¿Con qué criterios comparamos las leyes de protección de datos de América Latina? **34**
Delegado de protección de datos personales 34
Responsables y encargados de tratamiento 36
Derechos 38
Autoridad de aplicación 39
Transferencias internacionales 40
El impacto de GDPR en las leyes de protección de datos de América Latina y el Caribe **41**
Conclusiones **46**
Bibliografía **51**

ANEXO I: "Codebook de variables para el análisis cuantitativo de las leyes de protección de datos personales de América Latina y el Caribe" 52
ANEXO II: Tablas con composición de índices 90
ANEXO III: Base de datos sobre leyes de protección de datos en América Latina y el Caribe 96

Introducción

El presente estudio tiene como objeto realizar un análisis profundo de la protección de datos personales en América Latina y el Caribe. El análisis se enfoca mayormente en la dimensión *de iure* de la protección, tomando como unidades de análisis a las 19 leyes de protección de datos personales que han sido sancionadas hasta el momento en América Latina y el Caribe. Se tomó como horizonte normativo a la Regulación General de Datos Personales de la Unión Europea (GDPR, por sus siglas en inglés), a partir de la cual se formuló un marco metodológico compuesto por 160 variables y 7 índices. Partiendo de dicho marco metodológico se condujeron diversos análisis estadísticos.

Se aportó evidencia empírica robusta a favor de la existencia de grupos de leyes con características parecidas en la región. Para testear la primera hipótesis, la cual propone que *"no hay un marco regulatorio homogéneo respecto a la protección de datos personales en América Latina, sino que existen grupos de regulaciones de datos personales que cuentan con distintas características"*, se realizó un análisis de clúster. Existe un grupo de leyes con una baja protección de datos personales, compuesto por Paraguay, Chile, Antigua y Barbuda, República Dominicana y Cuba. Estos países tienen leyes con pocas exigencias a los responsables y encargados de tratamiento, reconocen pocos derechos digitales, tienen autoridades extremadamente endebles o inexistentes, y tienden a contener pocas o ninguna regulación a la transferencia internacional de datos personales. Existe también un grupo de leyes con una buena protección de derechos digitales, compuesto por Argentina, Colombia, Costa Rica, México, Nicaragua, Panamá, Perú, Saint Kitts y Nevis y Uruguay. Este grupo de leyes reconoce, en promedio, una mayor cantidad de derechos digitales que la amplia mayoría de los países de la región. El tercer grupo está compuesto por Brasil, Santa Lucía y las Bahamas, y es el grupo de leyes con autoridades robustas. Este grupo se destaca por sobre el resto por tener autoridades independientes, con amplios poderes informativos y

coercitivos, y con injerencia por sobre el proceso legislativo en torno a la protección de datos personales. Por último, el grupo de leyes abarcativas, compuesto por Ecuador y Barbados, se caracteriza por tener leyes con una alta protección de datos personales en múltiples aspectos, incluyendo incluso instrumentos de protección novedosos introducidos en GDPR, tales como el derecho a no ser sujeto de decisiones automatizadas y el derecho a la portabilidad, entre otros.

Se aportó evidencia muy sólida a favor de la hipótesis de que los países de la región de América Latina y el Caribe están emulando activamente el articulado de GDPR. Con el objetivo de testear la segunda hipótesis, *las leyes sancionadas post 2016 se dieron mayormente influidas por GDPR y el modelo de la Commonwealth*, se diseñó un modelo de regresión lineal múltiple. En el mismo se tomó en consideración la población total de los países estudiados, su nivel de democracia, si eran federales o unitarios, y si pertenecían a la Commonwealth. Estas variables fueron introducidas al análisis para controlar por variables intervinientes.

¿Por qué hablamos de datos personales?

Vivimos en la era de la información. A lo largo de los 10 últimos años la cantidad de datos generados almacenados y distribuidos ha crecido exponencialmente, al punto de obligar al Comité Internacional de Pesas y Medidas a crear nuevos términos para dar cuenta del volumen de los datos existentes.[1]

Existen numerosos estudios que han intentado cuantificar la cantidad exacta de datos generados en la última década, y no se ha logrado un consenso en esta rama de la literatura. Sin embargo, sí

[1] Kitchin, R. (2014). *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences*. SAGE.

existe un acuerdo en torno a la existencia de un proceso de *datificación*[2]. El mismo refiere a un movimiento de la industria y de los estados a intentar capturar y generar cada vez más datos. Cada día se publican más de 400 millones de tweets, cada uno de los cuales tiene de 33 ítems discretos de metadata[3]. A su vez, gobiernos e instituciones públicas generan vastas cantidades de datos sobre sus ciudadanos: entidades reguladoras del tránsito monitorean las personas que usan los sistemas de transporte, y aplicaciones y medios online de pago de impuestos capturan información financiera sobre sus usuarios[4]. Si bien esta información puede ser utilizada para generar avances científicos tecnológicos y descubrimientos sociales y económicos, también puede ser utilizada para fines de control social y violaciones a Derechos Humanos[5]. Es por eso que desde la ciencia política debemos prestar atención a la manera en la cuál los Estados legislan en torno a los datos, y en particular a los datos personales.

Los datos personales son de especial interés a la hora de estudiar la forma en la que los Estados se aproximan a los datos en general, debido a que explotarlos de manera indebida vulnera los derechos a la privacidad de la ciudadanía. Según la Regulación General de Datos Personales de la Unión Europea, un dato personal es "toda información sobre una persona física identificada o identificable [...]; se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o

[2] Mikołajska, A. (2015). Viktor Mayer-Schönberger, Kenneth Cukier, BIG DATA: rewolucja, która zmieni nasze myślenie, pracę i życie, przeł. M. Głatki, Warszawa: MT Biznes 2014, s. 280. *Biblioteka*, *19(28)*, 267. https://doi.org/10.14746/b.2015.19.18

[3] Ibíd., p. 3 (Kitchin).

[4] Ibíd., p. 3 (Kitchin).

[5] Ibíd., p. 3 (Mikołajska).

varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;"[6]

A los fines de brindar contexto a la presente investigación, en la siguiente sección se dedicarán algunos párrafos al análisis de la historia reciente de la protección de datos personales, enfatizando en el marco regulatorio europeo y en su influencia a lo largo de los años en las leyes latinoamericanas.

La influencia de la regulación de privacidad de datos personales europea en las leyes de América Latina y el Caribe no es un fenómeno novedoso, ni que se reduzca meramente a GDPR. Por el contrario, la influencia transnacional del marco regulatorio europeo se remonta a 1995[7]. En dicho año se aprobó la Directiva 95/45EC[8] respecto de la protección de los individuos con respecto al procesamiento de los datos personales y su transferencia.[9]

Una rama de la literatura sobre el análisis del marco regulatorio europeo sobre protección de privacidad de datos personales y su influencia en las leyes del resto del mundo señalan que es en América Latina donde el proceso de influencia transnacional de la Unión Europea puede verse más

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1

[7] Brown, I. (2013). *Research Handbook on Governance of the Internet*. Edward Elgar Publishing.

[8] OPOCE. (1995, 23 noviembre). *Directiva 95/45 EC*. Recuperado 10 de julio de 2023, de https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046

[9] Carrillo, A. J., & Jackson, M. (2022). Follow the Leader? A Comparative Law Study of the EU's General Data Protection Regulation's Impact in Latin America. *ICL online journal*, *16*(2), 177-262. https://doi.org/10.1515/icl-2021-0037

claramente[10]. Un ejemplo de ello es el hecho de que desde 2016, año en el cual se aprobó GDPR, 16 países de la región han debatido o incluso adoptado nuevas leyes de protección de datos personales[11]. En este sentido, GDPR emerge como un ejemplo del proceso global de convergencia de políticas al cual Anu Bradford llama "Efecto Bruselas". Este proceso, según Bradford, consiste en un instrumento de poder de la Unión Europea, la cual logra a través de la extraterritorialidad imponer "de facto" regulaciones análogas a la suya en el resto del mundo.[12]

Respecto de los medios a través de los cuales la Unión Europea ejercita dicha influencia, hay un debate en la literatura en torno a cuáles son los mecanismos empleados. Por un lado, autores y autoras como Bradford indican que este proceso de influencia se dio a través de mecanismos de mercado, a través de los cuales Europa fue capaz de exportar "unilateralmente" los marcos legales a otra jurisdicciones[13]. Esta transferencia de piezas normativas fue acogida por los países de América Latina "*de jure*" a través de la sanción de leyes en sintonía con aquellas del viejo continente, así como también "de facto" con el objetivo de cumplir con los estándares propuestos por Europa para que las empresas extranjeras puedan brindar servicios en la Unión Europea.

Otro cuerpo de literatura propone que en realidad Europa ha utilizado múltiples instrumentos de negociación y estrategias que facilitaron la divulgación de sus leyes de protección de datos personales.[14]

---

[10] Greenleaf, G. (2012). The influence of European data privacy standards outside Europe: implications for globalization of Convention 108. *International Data Privacy Law*, *2*(2), 68-92. https://doi.org/10.1093/idpl/ips006

[11] Los países son Argentina, Brasil, Bolivia, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Guyana, Honduras, Panamá, Paraguay, México, Surinam, y Uruguay. Ver cita 8.

[12] Bradford, A. (2020). *The Brussels Effect: How the European Union Rules the World*. Oxford University Press.

[13] Ibíd.

[14] Schwartz, P. M. (2019). *Global Data Privacy: The EU Way*.

En suma, existen libros y artículos que analizan la manera en la cual los países de América Latina han realizado el proceso de incorporación de las innovaciones que trajo GDPR a sus propios marcos legales. Carrillo y Jackson señalan que la misma se dio a través de procesos de enmienda de las leyes preexistentes, y no tanto a través de la sanción de nuevas disposiciones legales. En suma, los autores agregan que el proceso de réplica de GDPR se vio complementado por la adhesión de algunos de los países de la región a la Convención 108+[15] [16].

Sin embargo, la manera más robusta de argumentar la incorporación de elementos clave del articulado de GDPR por parte de los países de América Latina y el Caribe es mediante el estudio de la presencia de dichos elementos en cada una de las leyes de la región. Existen diferentes perspectivas respecto a cuáles son dichos elementos centrales de la nueva legislación Europea, pero en el presente estudio se ha tomado en cuenta todas estas diversas opiniones para poder dar con una evaluación de la similitud de las leyes de la región con aquella de Europa lo más completa posible.

¿Cómo se protegen los datos personales?

Para comprender la manera en la que se legisla en torno a los datos personales, es menester reconocer su carácter dual. Una rama de la literatura[17] señala que los instrumentos que componen los marcos legales que regulan la recolección, almacenamiento y tratamiento de los datos personales pueden categorizarse según si son predominantemente basados en derechos u

[15] *Convention 108+*. (2008, junio). Council of Europe. Recuperado 10 de julio de 2023, de https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

[16] Ibíd., p. 5 (Carrillo & Jackson).

[17] e.g., Murray, A. M. (2019). Data as a Commodity vs Data as a Right. *Policy paper, LSE*. & Rauhofer, J. R., & Lynskey, O. L. (2018). Review of Commonwealth modelo laws on data protection. *Edinburgh: University of Edinburgh School of Law*.

orientados al mercado. A su vez, el hecho de que los marcos regulatorios puedan centrarse en dos componentes distintos es lo que da cuenta de la dualidad del dato: un dato puede ser visto al mismo tiempo como información que se beneficia de la protección de derechos fundamentales, y como un bien explotable económicamente[18]. En esa lógica, GDPR es una ley predominantemente basada en derechos. [19]

En los siguientes párrafos se analizarán cuáles son algunos de los pilares que sostienen y organizan el articulado de GDPR, con la intención de introducir al lector a los instrumentos de protección de datos personales. Pero antes me gustaría señalar que cada ley de protección de datos personales es fruto de un proceso propio de formulación de política pública, y que por lo tanto no existen dos leyes iguales (aunque si argumentaré más adelante que existen grupos de leyes llamativamente similares). Lo que quiero decir es que no todos los articulados se estructuran de igual manera, y que por ende la lista de elementos que encontrará el lector a continuación es meramente enunciativa.

Derechos

Retomando la idea de que los datos son, al menos en una de sus dimensiones, información plausible de verse beneficiada por la protección de derechos fundamentales, las leyes de protección de datos suelen consagrar derechos para los titulares. Los titulares son las personas sujeto de los datos recolectados sobre los que aplican estas leyes.

Los derechos reconocidos en este tipo de instrumentos legales, y sobre todo en los que emulan a GDPR, suelen brindar al titular la facultad de ser informado respecto a sus derechos o características del tratamiento al que se someterán sus datos personales; conceder al titular la

[18] Murray, A. M. (2019). Data as a Commodity vs Data as a Right. *Policy paper, LSE*.

[19] Rauhofer, J. R., & Lynskey, O. L. (2018). Review of Commonwealth modelo laws on data protection. *Edinburgh: University of Edinburgh School of Law*.

prerrogativas de acceso, rectificación, cancelación u oposición al tratamiento (conocidos como derechos ARCO por sus siglas); o reconocen garantías que amplían los poderes de los titulares por sobre sus datos en otras maneras tales como el derecho a la portabilidad o derecho a no ser sometido a decisiones automatizadas. En particular, estos últimos fueron algunas de las novedades introducidas por GDPR.

Instrumentos

Las leyes de protección de datos brindan a los titulares herramientas para hacer valer sus derechos y obligar a los responsables de tratamiento y autoridades de control al correcto ejercicio de sus funciones. Estas herramientas pueden ser legales (tales como el habeas data o procesos judiciales), administrativas (iniciar procedimientos frente a la autoridad de control), o pueden implicar la terceras figuras a las cuales el titular puede recurrir para asesorarse.

Consideraciones respecto del consentimiento

Múltiples son las leyes de protección de datos personales que realizan algún tipo de observación respecto del consentimiento del titular. Algunas de ellas demandan el consentimiento del titular como una condición para la legalidad del tratamiento. Otras establecen un umbral de edad mínima para brindar consentimiento. También existen aquellas que exigen al responsable que brinde la posibilidad de retirar el consentimiento de forma sencilla.

Transferencias internacionales

La transferencia transfronteriza de los datos personales recolectados suele estar regulada por las leyes de datos. En este sentido, los Estados buscan brindar garantías a los titulares de los datos respecto a la seguridad y la integridad de sus datos. Las leyes suelen enunciar condiciones que determinan la legalidad de las transferencias. Estas suelen incluir la existencia de leyes de protección de datos o autoridades de control en el país de destino y la existencia de tratados internacionales relevantes, entre otras.

Responsable de tratamiento

Las leyes de protección de datos personales suelen reconocer la existencia de una persona responsable legalmente por los procesos de recolección, tratamiento y almacenamiento de los datos. Esta persona, usualmente llamada responsable o controlador (*controller*), suele ser sujeta a exigencias respecto de sus funciones.

Las leyes suelen exigir a los responsables de tratamiento que implementen medidas de seguridad para asegurar la integridad de los datos y condiciones para la contratación de terceros encargados de tratamiento. A su vez, algunas leyes exigen a los responsables que notifiquen a los titulares o a las autoridades ante una vulneración de la seguridad de los datos.

Delegado de protección de datos (Data Protection Officer):

Esta figura, introducida por primera vez por GDPR, refiere a una persona designada del padrón de empleados de las empresas, a quien se le otorga la responsabilidad de llevar a cabo las tareas de supervisión y control de los tratamientos efectuados. A diferencia del encargado (*data processor*), quien suele ser un tercero externo a la empresa a quien se contrata para llevar a cabo las tareas de tratamiento y asegurarse de cumplir con los estándares adecuados, el DPO es una persona contratada con una posición fija en la empresa a quien la ley suele otorgar prerrogativas tales como independencia en su accionar. A su vez, suele ser impuesto como una exigencia a entidades que realicen determinados tipos de tratamientos, tales como tratamientos a gran escala o en espacios públicos.

Autoridad de aplicación

Son numerosas las leyes de protección de datos que designan o crean una autoridad de aplicación. Esta es la institución o entidad pública encargada de hacer cumplir la ley, y se le suelen otorgar un conjunto de prerrogativas informativas (demandar acceso a base de datos, iniciar procesos de

auditoría, etc), coercitivas (multar a responsables por sus infracciones, iniciar procesos administrativos, etc) o de asesoramiento a otros cuerpos del Estado. A su vez algunas leyes definen su competencia, la cual puede incluir dar lugar y responder ante los reclamos de los titulares de datos.

En mi carácter de politólogo presté especial atención a las características institucionales de estas autoridades: ¿son entes independientes, u oficinas de otros ministerios? ¿Se les asigna un presupuesto anual, o su financiamiento está sujeto a otros actores? ¿Su responsable es designado a través de procesos de selección predeterminados, o es puesto en el cargo a discreción por otro actor?

Marco metodológico

Las hipótesis que condujeron este estudio fueron dos:

> *H1: no hay un marco regulatorio homogéneo respecto a la protección de datos personales en América Latina, sino que existen grupos de regulación de datos personales que cuentan con distintas características.*

> *H2: las leyes sancionadas post 2016 se dieron mayormente influidas por GDPR y el modelo de la Commonwealth*[20]*.*

Al momento de diseñar las variables que serían utilizadas para el estudio, se decidió que se buscaba evaluar tanto la presencia como ausencia de elementos de la protección de datos personales en las leyes de América Latina. Es por ello que se consideró necesario construir las variables a partir de la ley con una protección de datos personales más elevada de la que se tiene conocimiento: la Regulación General de Datos Personales de la Unión Europea (GDPR). Con una buena protección de datos personales nos referimos a la extensión e intensión de una ley: una ley con un nivel elevado de protección es aquella que contempla numerosas aristas de la privacidad, atendiendo a lo público y a lo privado, reconociendo numerosos derechos, favoreciendo la creación de mercados, y más.

A partir del texto de GDPR, se estudió el articulado y se procedió a la confección de 160 variables dicotómicas, las cuales buscan medir en otras leyes la existencia de disposiciones similares a las

[20] La Mancomunidad de Naciones es una organización de países con lazos históricos con el Reino Unido de Gran Bretaña e Irlanda del Norte. En 2022, la Commonwealth publicó una ley modelo de protección de datos.

de GDPR. Se elaboró un codebook[21], el cual contiene toda la información relevante respecto de las variables.

A continuación, se seleccionó el conjunto de leyes a ser estudiadas. Por motivos de interés teórico, se decidió circunscribir el estudio a la región de América Latina y el Caribe. Se investigó cuidadosamente el marco normativo de cada país de la región respecto a la temática de datos personales, encontrando que tan solo 19 de los países de la región cuentan con leyes sancionadas[22]. Otros países cuentan con conjuntos de decretos presidenciales que regulan la cuestión, pero por criterios metodológicos se decidió avanzar solamente con aquellos Estados que contaban con cuerpos legales aprobados por legislaturas. Siendo que las leyes de protección de datos personales de la región no representan una población lo suficientemente grande, se optó por integrar a todas en el estudio para robustecer los métodos estadísticos conservando la muestra *(n)* lo más grande posible. En este caso, la "muestra" integra todos las unidades de la población de interés ($n = N$).

A medida que se estudiaban las leyes, se construyó una base de datos en la que se tomó registro de los valores de las variables diseñadas, dando cuenta de las características y la composición de las leyes de Latinoamérica y el Caribe, su nivel de protección de los datos personales y, por cómo se diseñaron las variables, su nivel de similitud con GDPR. Esto último se debe a que las variables se construyeron únicamente a partir de elementos presentes en GDPR. Al ser dicotómicas, las variables permiten que la suma de sus valores represente un índice de cuán similares son a GDPR. En consecuencia, y al considerar que este estudio utiliza GDPR como un horizonte normativo respecto al nivel de protección de las leyes de protección de datos personales, ese mismo índice da cuenta del nivel de la protección de los datos personales en cada una de las leyes de América Latina y el Caribe.

[21] Un codebook es un documento que contiene toda la información de las variables utilizadas: su nombre, código, la información que busca medir, el nivel de medición (nominal, ordinal, intervalar), y la fuente en el caso de que se usen variables de otra base de datos.

[22] Estos países son Antigua y Barbuda, Argentina, Bahamas, Barbados, Chile, Colombia, Costa Rica, Cuba, Ecuador, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Saint Kitts y Nevis, Santa Lucía y Uruguay

Al concluir con la revisión de las leyes, nos propusimos confeccionar índices. La indización de variables, según Ansolabehere, Rodden y Snyder, permite mejorar la calidad de la medición. Esto se debe a que los errores aleatorios y de medición son inherentes a investigaciones como la presente. Al generar un índice y comparar las leyes a partir de los mismos, se reduce el impacto de los errores de medición en los resultados del estudio, permitiendo así comprender mejor el fenómeno estudiado. Para decidir cuáles serían los índices utilizados nos basamos en conceptos teóricos: siendo que los índices se utilizarían para comparar clústers entre sí, nuestro interés era que los puntos de comparación y contraste fueran elementos generales de la protección de datos. En ese sentido, acudimos a la bibliografía y a los ejes que organizan el articulado de GDPR para comprender mejor cuales son los conceptos principales en torno a los cuales guiar la comparación. El resultado fueron los siete índices expuestos a continuación.[23]

Índice de Consentimiento

Este primer índice tiene como objetivo comprender cuán amplias son las exigencias que la ley pone a los responsables en torno al consentimiento que brinda el titular para el tratamiento de sus datos. Está compuesto por tres variables, las cuales buscan medir si la ley define que el consentimiento debe ser brindado en un contexto de fácil acceso que presente lenguaje claro, si la ley exige que el consentimiento pueda ser retirado de forma sencilla, y si establece una edad mínima a partir de la cual una persona puede dar consentimiento.

Índice de Derechos

Este índice, compuesto por 18 variables, intenta medir cuántos derechos son reconocidos por la ley. Observa derechos a ser presentado con información sobre el tratamiento al momento de brindar el consentimiento, derechos ARCO y derechos a conocer características del tratamiento, entre otras.

[23] En el anexo el lector podrá encontrar una tabla detallando las variables que componen cada uno de los índices, junto a sus descripciones.

Índice de Instrumentos

Busca analizar cuáles son las prerrogativas de los titulares para utilizar instrumentos administrativos, legales y judiciales para hacer valer sus derechos. Se compone de 7 variables.

Índice de Responsable de tratamiento

Con el objetivo de medir en qué medida la ley asigna responsabilidades y obligaciones a los responsables y encargados de tratamiento, se construyó un índice con 9 variables. Estas miden si la ley crea las figuras de responsables, encargados[24] y representantes[25]. A su vez, observan si estos deberán notificar a autoridades y titulares en caso de una violación a la integridad de los datos personales, y si deberán conducir evaluaciones de impacto[26].

Índice de Delegado de protección de datos

Este índice, compuesto por 7 variables, busca medir la presencia de artículos que creen una figura análoga a aquella del delegado de protección de datos (*data protection officer*). Adicionalmente, estudia en qué situaciones la ley exige al responsable la designación de un DPO.

Índice de Transferencias internacionales

Compuesto por 6 variables, este índice estudia la presencia de artículos acerca de las transferencias internacionales. Hace especial hincapié en las decisiones de adecuación. Estas son decisiones que

[24] Los encargados de tratamiento son aquellas personas ajenas a la empresa o establecimiento, a quien el responsable recurre para que lleve a cabo tareas relacionadas al tratamiento de los datos personales

[25] El representante es una persona encargada de representar al responsable en los casos en que este no vive en el país

[26] Las evaluaciones de impacto son estudios que debe realizar un responsable antes de conducir el tratamiento. Dicha evaluación tiene como objetivo identificar los posibles riesgos o vulnerabilidades del tratamiento

debe tomar la autoridad de aplicación para definir si los responsables tienen permitido transferir datos personales a terceros países.

Índice Autoridad de aplicación

Este índice es singularmente grande, conteniendo 23 variables. Las mismas buscan medir el grado de independencia de la autoridad de aplicación designada o creada por la ley, sus poderes, responsabilidades y prerrogativas.

Continuamos con el diseño de métodos estadísticos para testear las hipótesis de investigación. Para testear la hipótesis 1, *"no hay un marco regulatorio homogéneo respecto a la protección de datos personales en América Latina, sino que existen grupos de regulaciones de datos personales que cuentan con distintas características"*, decidimos llevar adelante un análisis de clúster para comprender mejor cómo se agrupan las leyes. Se usaron como variables los índices presentados en el párrafo anterior.

Por último, se realizó una regresión lineal para evaluar la segunda hipótesis: *"las leyes sancionadas post 2016 se dieron mayormente influidas por GDPR y el modelo de la Commonwealth*". Al contar con el índice de nivel de protección de datos personales, que a su vez representa el grado de similitud entre cada una de las diecinueve leyes y GDPR, se logró diseñar un modelo de regresión lineal que evalúa si el hecho de haber sido sancionada antes o después de 2016 (año de publicación de GDPR) contribuye a explicar que una ley tenga un mayor nivel de protección de datos. Se incluyeron en el modelo otras variables de interés que creímos que contribuirían a controlar por variables intervinientes para así evitar relaciones espuria[27].

[27] Las variables de control fueron el índice de democracia, el tipo de régimen, la pertenencia a la Commonwealth y la población del país en 2019.

El análisis conducido permitió relevar cuáles son las condiciones con las que cumplen la gran mayoría de las leyes de la región. Reconocer este punto permite abordar el estudio de los estándares básicos de la protección de datos en América Latina. Describiré cuáles son estos estándares en las siguientes tres secciones.

Datos como bien: facilitando un mercado

Lynskey y Rauhofer[28] señalan que GDPR es un ejemplo de una ley orientada según un enfoque que caracteriza a los datos como derechos. En este sentido, al analizar la dualidad del dato es esperable que, habiendo operacionalizado variables con GDPR como base, hallemos que las leyes de protección de datos de la región tengan esta misma orientación. Sin embargo, esto no implica la invalidación del hallazgo sino que señala la subrepresentación de los componentes que podrían dar a las leyes de la región una orientación de mercado. En este aspecto, algunas de las variables utilizadas para medir las leyes analizadas forman parte de lo que Murray[29] señala como características de las leyes orientadas al mercado.

En cuanto a las dimensiones económicas de los estándares de la protección de datos en América Latina, y teniendo en cuenta lo mencionado en el párrafo anterior, fueron medidas numerosas variables que responden al escrutinio de dichas dimensiones. Sin embargo, una primera revisión de los datos revela que ninguna de estas variables midió un valor positivo para más de dos países de la región. En su paper, Lynskey y Rauhofer[30] sugieren que la existencia de criterios comunes para la autorización de transferencia transfronteriza de los datos pueden ser considerados parte de la dimensión económica de los datos. A diferencia de las otras variables de esta dimensión, TRANSF_EXIST mostró valores positivos para 16 de las 19 unidades.

[28] Ibíd., p. 7 (Rauhofer & Lynskey)
[29] Ibíd., p. 7 (Murray)
[30] Ibíd., p. 7 (Rauhofer & Lynskey)

Tal como indica la Directiva sobre protección de datos de la Unión Europea, con las sucesivas leyes de protección europeas se ha buscado como uno de los objetivos facilitar el libre movimiento de datos personales en la Unión[31]. Y es que, si bien GDPR es una ley predominantemente centrada en la protección de derechos fundamentales[32], el diseño de GDPR también contribuye a la creación de un mercado de datos, estableciendo normas compartidas y estándares comunes, permitiendo así el alineamiento de las expectativas y la coordinación de medidas de seguridad. En este sentido, 12[33] de las leyes analizadas plantean que la transferencia a terceros países requiere una decisión de adecuación. Sin embargo, solo 4 de las leyes analizadas demandan considerar la existencia y características de leyes de protección de datos en los terceros países para dar lugar a la transferencia a terceros países[34].

Datos como derecho, usuario como sujeto

A la hora de explicar cuáles son las características de una ley que constituyen a los titulares como verdaderos sujetos de derecho por sobre sus datos, es difícil quedarse con tan solo algunas de las variables estudiadas. Sin embargo en esta sección se subrayan un conjunto de características a las que consideramos elementales a la hora de pensar los datos como un derecho. Estas son la minimización de los datos, el consentimiento y el derecho a conocer el tratamiento.

La minimización de los datos recogidos es un diseño institucional que evita que el titular de los datos sea visto como un mero conjunto de *data points* a ser escrutado y explotado. La minimización suele operar de forma tal que circunscribe la recolección de datos a aquellos que son absolutamente necesarios para la consagración del objetivo declarado del tratamiento. De esta manera, una

[31] Ibíd., p. 7 (Murray)
[32] Ibíd., p. 7 (Rauhofer & Lynskey)
[33] Estos países son Argentina, Bahamas, Barbados, Brasil, Colombia, Ecuador, México, Nicaragua, Panamá, Perú, Saint Kitts y Nevis y Uruguay.
[34] Estos países son Brasil, Ecuador, Barbados y Santa Lucía.

decisión que se toma antes de comenzado el tratamiento circunscribe cuáles serán las categorías de datos plausibles de ser recolectadas. En el caso de América Latina y el Caribe, solo son 9 los países que cuentan con artículos que aseguran la minimización de los datos[35].

Otra característica fundamental a la hora de pensar al titular como un sujeto de derecho es el tratamiento basado en el consentimiento. Nos detendremos en este punto y analizaremos algunas de las consecuencias prácticas de este diseño institucional. En primer lugar, la inclusión de artículos de esta índole tienen una implicancia fundamental para este análisis: hacen que el tratamiento no sea lícito por *default*. En segundo lugar, esta característica logra acortar la brecha de poder entre el titular y las plataformas. Si bien este tipo de cláusulas no brinda derechos de propiedad al titular por sobre sus datos, de alguna forma le permiten controlar qué datos son recolectados, para qué fines y quién hará uso de los mismos. La medición conducida revela que son 17 los países que integran este tipo de cláusulas.[36]

En tercer lugar, me parece fundamental destacar el rol de los Derechos a la información sobre el tratamiento a la hora de consagrar al titular como sujeto de derecho. La presencia de dichos derechos fue medida en el estudio mediante la variable DS_R_TRTMT, la cual midió valores positivos para 17 de los 19 países estudiados[37]. La misma respondía a la pregunta "¿Tiene el interesado derecho a obtener información sobre el tratamiento de sus datos personales?". Esta variable aglomera distintos tipos de características sobre las cuales el interesado podría requerir información: el objeto, los destinatarios, decisiones automatizadas, etc. Brindar este tipo de derechos a los titulares de los datos es una manera de generar un contrapeso al amplio poder de las plataformas, dado que habilita pedidos de rendición de cuentas por parte de los titulares de los miles de millones de puntos de datos que poseen los responsables del tratamiento. Es esta

[35] La existencia de estos artículos se midió con la variable TRTMT_PRINC3, y los países que cuentan con artículos de esta índole son: Bahamas, Barbados, Brasil, Ecuador, México, Nicaragua, Panamá, Saint Kitts y Nevis y Santa Lucía.
[36] Las leyes de Bahamas y Paraguay son las únicas que no incluyen este tipo de artículos.
[37] Las leyes de Paraguay y República Dominicana son las únicas que no incluyen este tipo de artículos.

característica en particular la que da lugar a procesos de *accountability* que pueden derivar en el descubrimiento de errores, equivocaciones e incluso abusos por parte de los responsables.

Reafirmando el derecho del titular por sobre sus datos

Las cláusulas descritas en el inciso anterior brindan al titular de los datos un poder por sobre sus datos que podría ser descripto como pasivo: los usuarios tendrán derecho a que no se recolecten datos de más, a que no sean tratados o recolectados sin su consentimiento y a, en caso de así requerirlo, ser informado acerca de las características básicas del tratamiento de los mismos. Los derechos descritos en esta sección responden a otro orden de características: habilitan al titular a tener control activo sobre sus datos.

El principio de exactitud de los datos, el cual figura en todas las unidades de análisis comprendidas en el estudio cuantitativo llevado a cabo, sirve como base legal para los derechos ARCO. La variable utilizada para medir la presencia del principio de exactitud fue TRTMT_PRINC4, la cuál evalúa si la ley estipula que los datos serán a exactos y, si fuera necesario, actualizados.

Los derechos de limitación del tratamiento y supresión o rectificación de los datos fueron hallados en las 19 unidades de análisis estudiadas. Este es un punto en el que deseo hacer hincapié, debido a que habla muy bien del estándar mínimo de protección de datos en América Latina y el Caribe. Estos derechos reafirman la titularidad de los datos por parte del interesado, y sirven como premisa para afirmar que en América Latina y el Caribe los datos personales son concebidos como más que un bien, al menos *de iure*. Muchas de las leyes analizadas incluso profundizan en este punto, estipulando con claridad los pasos a seguir por parte del titular de los datos, y las obligaciones del responsable del tratamiento.

La protección de datos conlleva medidas de seguridad y obligaciones:

Tal como se argumentó en las secciones anteriores, la creación de obligaciones para con los titulares por parte de los responsables de tratamiento contribuye a subsanar la diferencia de poder que existe hoy entre los responsables y los usuarios. En este sentido, a la hora de analizar el estándar latinoamericano y del Caribe de protección de datos, es fundamental tener este tipo de cláusulas en cuenta.

La variable utilizada para medir si la ley estipula que los datos serán tratados de forma que se garantice su seguridad y se prevenga su pérdida fue TRTMT_PRINC6. En la mayoría de los casos, estas variables no cuentan con cláusulas operacionalizadas que denoten las prácticas específicas que se demandan a los responsables y encargados de tratamiento. No obstante, la presencia de este tipo de cláusulas es fundamental, dado que sientan las bases para la construcción de un articulado que garantice la integridad y la confidencialidad de los datos. La de Paraguay fue la única de las leyes estudiadas en no contar con este tipo de artículos.

Respecto a la creación de figuras legales, 18 de las 19 leyes estudiadas contemplaron la figura del responsable del tratamiento[38]. Esta figura es entendida como una persona física o jurídica que determina, sola o en conjunto con otras personas, los fines y los medios del tratamiento de datos personales. La existencia de esta figura es fundamental a la hora de estudiar el estándar de protección desde este enfoque, dado que crea una persona responsable, frente a la cual se pueden exigir el ejercicio y correcto cumplimiento de los derechos de los titulares de los datos personales. A su vez, 18 de las 19 unidades de análisis asignan a la figura del responsable del tratamiento la obligación de llevar a cabo medidas de seguridad que garanticen la integridad y confidencialidad de los datos recogidos tratados y distribuidos[39]. Incluso la gran mayoría de estas leyes exige a los

[38] La de Paraguay fue la única de las leyes estudiadas en no contar con la figura del responsable de tratamiento.
[39] La de Paraguay fue la única de las leyes estudiadas en no exigir medidas de seguridad al responsable de tratamiento.

responsables que las medidas de seguridad sean puestas en ejercicio en todas las etapas del tratamiento, contribuyendo así a un procesamiento de datos seguro desde el diseño[40].

Continuando con el estudio de la existencia y consecuencias prácticas de las figuras establecidas en las leyes de protección de datos estudiadas, es interesante señalar que 17 de los casos estudiados disponen de la creación o designación de una autoridad de aplicación[41]. Esto es un punto central a la hora de comprender cuál es el nivel de protección en América Latina y el Caribe, debido a que la creación o designación de autoridades de aplicación para las leyes de protección de datos da cuenta de una obligación del Estado. En este sentido, la designación de presupuesto, la creación de equipos, la creación de procesos administrativos, y demás elementos contenidos en la mayoría de las cláusulas que refieren a la designación o creación de una autoridad de implementación de estas leyes generan una responsabilidad ineludible al estado. Este último punto puede ser tomado como un indicador de la medida en la protección de datos ha logrado insertarse en la agenda de las agencias estatales en América Latina y el Caribe.

[40] Ver artículo 25 de GDPR, “Protección de datos desde el diseño y por defecto”.
[41] Las leyes de Paraguay y República Dominicana son las únicas que no crean o designan una autoridad de aplicación

Índice de Protección de Datos Personales de América Latina y el Caribe

Tabla 1

Índice de Protección de Datos Personales en América Latina y el Caribe

Posición	País al que corresponde la ley de datos personales	Índice de Protección de Datos Personales de América Latina y el Caribe
1	Barbados	98
2	Ecuador	92
3	Santa Lucía	70
4	Brazil	65
5	Mexico	63
6	Peru	60
7	Saint Kitts y Nevis	58
8	Panama	56
9	Bahamas	55
10	Uruguay	54
11	Colombia	51
12	Nicaragua	50
13	Argentina	49
14	Costa Rica	48
15	Antigua y Barbuda	40
16	Chile	37
17	Cuba	35
18	República Dominicana	34
19	Paraguay	11

Nota: la presente tabla es de elaboración propia. El índice fue medido sobre un total de 160 variables, por lo que el resultado debe ser interpretado sobre un total de 160.

Tras el detenido análisis de las 19 leyes comprendidas en este estudio, se decidió agregar todas las variables en un solo índice, al que decidimos llamar "Índice de Protección de Datos Personales en América Latina y el Caribe", el cual se encuentra en la Tabla 1. El mismo refleja la medida en la cual cada una de estas leyes reconocen derechos a los titulares, asigna obligaciones a los responsables del tratamiento, crea o designa autoridades de aplicación robustas y regula las transferencias internacionales de datos personales. En suma, analiza la existencia de definiciones en torno a los ámbitos materiales y territoriales de las leyes, las excepciones que se realizan a pequeñas y medianas empresas, los principios sobre los cuales se basa la ley y otras características relevantes al nivel de protección de datos personales.

Con la confección de este índice se espera no sólo contribuir a la literatura académica en torno a la protección de datos personales en la región: pretendemos proponer un marco metodológico para seguir analizando y actualizando los marcos normativos en América Latina y el Caribe.

A través de un marco metodológico estandarizado se podrá analizar la evolución de las leyes de la región. A su vez, no sólo se podrá comparar las leyes en torno a su articulado, sino que la utilización del Índice de Protección de Datos Personales en América Latina y el Caribe permitirá analizar cuáles son las características legales de aquellas leyes que mejor desempeñan en la práctica[42]. Realizando análisis de los resultados de la protección de datos personales *de facto* y contrastándolos con los resultados del índice, se podrá brindar evidencia empírica robusta a favor de determinadas características o elementos de la protección de datos.

Por lo anteriormente mencionado, creemos que el Índice de Protección de Datos Personales en América Latina y el Caribe puede ser un buen instrumento para que la academia y las organizaciones de la sociedad civil que trabajan en torno a derechos digitales puedan realizar tareas de *assessment* constante del estado de la protección de datos en la región.

[42] Con protección de datos en la práctica se hacer referencia a la medida en la que se logran proteger los derechos digitales en la práctica. Indicadores de esto podrían ser cuántos juicios sobre derechos digitales se realizan por millón de habitantes, cuántas resoluciones administrativas expide una autoridad de aplicación, cuántas disputas legales gana un Estado frente a una plataforma digital, entre otras.

Destacamos la importancia que tiene la articulación entre la academia y las organizaciones de la sociedad civil. La protección de datos personales es una temática que presenta una considerable complejidad técnica, y es por ello que los actores involucrados deben trabajar en conjunto para crear y utilizar herramientas que logren asistir a los poderes legislativos de la región en la confección de leyes de protección de datos personales de avanzada.

¿Cómo encontramos los grupos de leyes de protección de datos personales?

Una vez terminado el estudio de las 19 unidades de análisis se procedió a realizar un análisis de clúster. Las variables que se midieron en las leyes fueron agrupadas en índices[43].

Una vez construidos los índices, se procedió a la aplicación de métodos jerárquicos de aglomeración[44] [45] con el objetivo de dilucidar si efectivamente existían clústers y, de haberlos, cuántos eran. La intención inicial fue aplicar métodos jerárquicos para comprender cuántos clústers hay y dar con una primera solución de aglomeración por clústers, basada en distancias euclídeas[46], y luego proceder a la realización de métodos no jerárquicos, utilizando distancias de

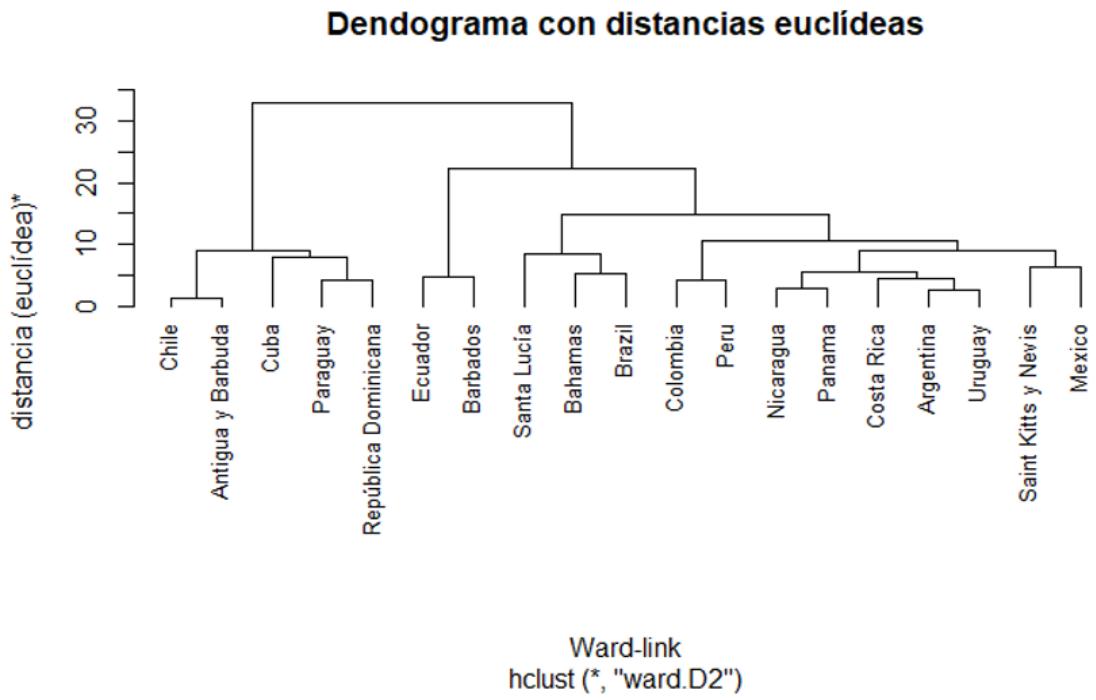
[43] Inicialmente se intentó realizar un análisis de componentes principales, pero la correlación de variables era muy baja, y los autovalores de los componentes rotados y sin rotar no eran lo suficientemente altos como para que fuese eficiente realizar el agrupamiento de variables por medio de este método.
[44] Los métodos jerárquicos de aglomeración, a diferencia de los no jerárquicos, sugieren a quien conduce el estudio la cantidad de clústers idónea a ser utilizada.
[45] Hair, J., Anderson, R., Black, B., & Babin, B. (2016). *Multivariate Data Analysis*. Pearson Higher Ed.
[46] Es una medida de distancia que se utiliza para calcular la distancia entre dos puntos en un espacio euclidiano, utilizando la fórmula de la distancia euclidiana, que es la raíz cuadrada de la suma de los cuadrados de las diferencias entre las coordenadas de los puntos.

Mahalanobis[47]. Por último, se decidió utilizar el método de K medias[48], para comparar con las soluciones anteriores y así evaluar cuán robustas es la solución hallada.

En primer lugar se utilizaron medidas de distancia euclídeas para el análisis, acompañadas de la utilización del método Ward[49]. El análisis inicial brindó como resultado un dendrograma con distancias euclídeas, expuesto en la Figura 1.

Figura 1

Dendograma utilizando distancias euclídeas



[47] Es una medida de distancia que tiene en cuenta la correlación y la varianza de las variables en un conjunto de datos multivariados, lo que permite considerar la estructura de los datos al calcular la distancia entre dos puntos.

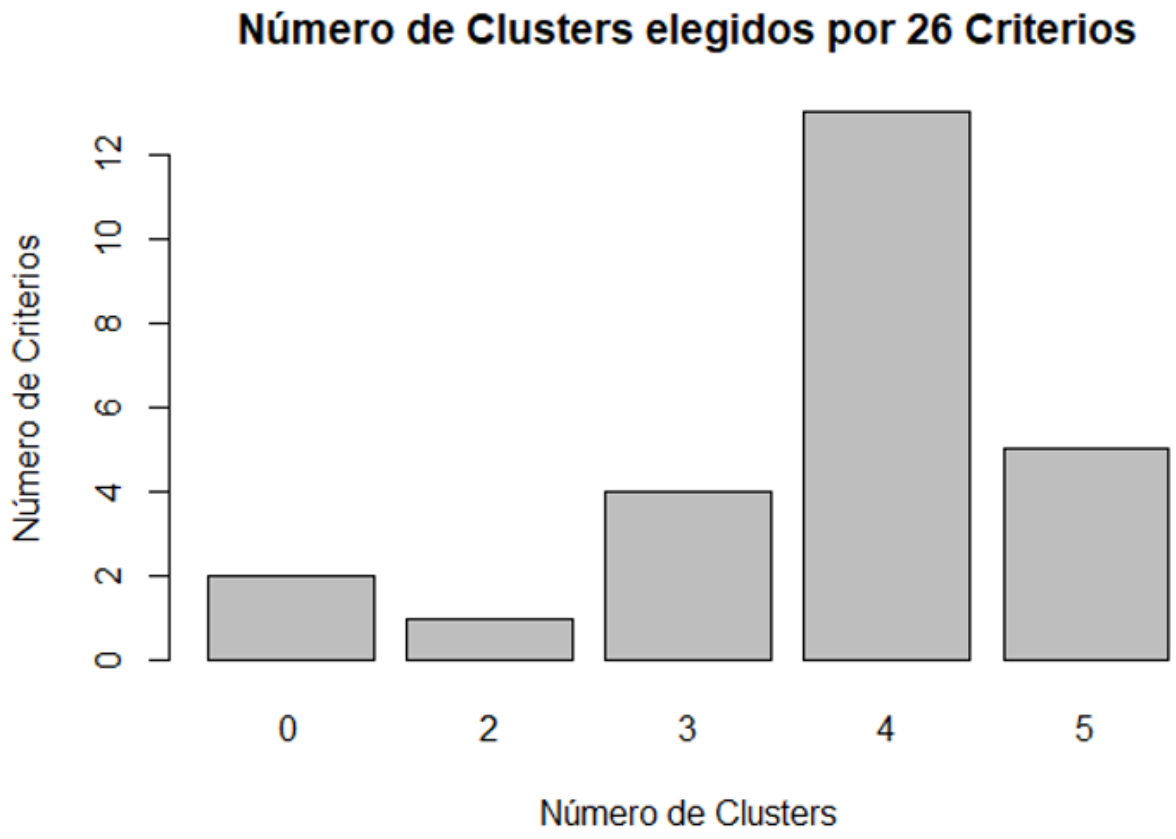
[48] Es un algoritmo de clústering que asigna puntos a K grupos, donde K es un número predefinido. El algoritmo calcula los centroides de los grupos y asigna iterativamente los puntos al grupo cuyo centroide está más cerca según una medida de distancia, como la distancia euclídea.

[49] Es un método de clústering aglomerativo que busca agrupar los puntos en clústers minimizando la suma de las varianzas dentro de los clústers. En cada paso, se fusionan los clústers que generan el menor incremento en la suma de varianzas, siguiendo una estrategia de aglomeración jerárquica.

Para determinar la cantidad de clústers se analizaron las sugerencias de 26 índices. De los 26 índices estudiados, 13 sugirieron la utilización de cuatro clústers. La distribución del total de las recomendaciones se encuentra expuesta en la Figura 2. De acuerdo con la regla de la mayoría el mejor número de clústers hallado fue 4, y por ello se decidió proseguir el estudio con dicha cantidad de clústers.

Figura 2

Histograma de Distribución de recomendaciones de cantidad de clústers



Al realizar el análisis de clúster utilizando método jerárquicos, distancia euclídea, método de Ward, y siguiendo las recomendaciones obtenidas del análisis de los 26 criterios mencionados anteriormente, se hallaron cuatro clústers con un gran grado de homogeneidad interna y heterogeneidad externa. Estos se encuentran expuestos en la Tabla 2.

Tabla 2

Leyes organizadas según clúster al que pertenecen

Clúster	Países a los que corresponden las leyes
Leyes con una baja protección de datos personales	Paraguay Chile Antigua y Barbuda Cuba República Dominicana
Leyes con una alta protección de derechos digitales	Costa Rica Argentina Nicaragua Colombia Uruguay Panamá Saint Kitts y Nevis Perú México
Leyes con autoridades de aplicación robustas	Bahamas Brasil Santa Lucía
Leyes abarcativas	Ecuador Barbados

Nota: tabla de elaboración propia.

Se analizaron los resultados de los indicadores de adecuación[50]. En particular se prestó atención a los resultados del índice CCC de adecuación, dado que sus resultados podrían brindar evidencia para la no existencia de clústers. Sin embargo, los resultados hallados brindan evidencia para la existencia de clústers, por lo que se decidió proseguir con el análisis, evaluando la fortaleza de los resultados.

Se procedió a la utilización de métodos no jerárquicos, puntualmente con distancias de Mahalanobis, y la realización del método de K Medias. El objetivo de estos pasos fue estudiar la robustez de la solución hallada por medio de la utilización de distancias euclídeas.

En primer lugar se analizaron los resultados de una aglomeración de 4 clústers usando distancias de Mahalanobis y método de Ward. A primera vista, los clústers obtenidos distribuyeron de forma similar las unidades de análisis. Sin embargo, la composición de los clústers cambió considerablemente. Esto se debe a que la distancia de Mahalanobis tiene en cuenta la covarianza de las variables a la hora de agrupar. Esto hace que los cambios en los resultados entre variables influyan en la aglomeración, haciendo posible que países que presentan distancias relativas entre los valores de distintas variables similares pero valores absolutos de esas variables muy distintos, puedan quedar agrupadas. Por este motivo, no tiene sentido teórico utilizar distancias de Mahalanobis para el estudio en cuestión. No obstante, hemos obtenido evidencia a favor de la existencia de cuatro clústers, debido a que la distribución del total de las unidades de análisis en los cuatro grupos ha sido similar para las dos medidas de distancia.

Por último, se utilizó el método de K Medias. Tras utilizar el número de cuatro clústers, se obtuvieron dos clústers absolutamente idénticos a aquellos obtenidos en la utilización de distancias euclídeas. Estos son los que fueron nombrados como “Leyes con una baja protección de datos

[50] Dunn, Pseudo T2, CCC y Pseudo F

personales", y el de "Leyes abarcativas". Los otros dos clústers fueron representados de forma similar por el método de K Medias, indicando que la solución hallada es robusta.

Se continuó el trabajo con los resultados obtenidos tras la utilización de distancias euclídeas.

¿Cuáles son los tipos de leyes de protección de datos personales en América Latina y el Caribe?

En la presente sección comenzaremos por realizar una descripción de las características de cada uno de los grupos de leyes, haciendo especial hincapié en aquellas que lo diferencian del resto. Luego, se realizarán algunas consideraciones generales de los resultados, para luego pasar a su análisis detallando los resultados de cada índice.

Leyes con una baja protección de datos personales

Este clúster se encuentra compuesto por las leyes de protección de datos personales de Paraguay, Chile, Antigua y Barbuda, Cuba y República Dominicana. Este grupo de leyes se caracteriza por presentar pocas exigencias a los responsables y encargados de tratamiento, reconocer pocos derechos digitales, tener autoridades extremadamente endebles o inexistentes, y tienden a contener pocas o ninguna regulación a la transferencia internacional de datos personales.

Uno de los hallazgos del análisis estadístico conducido es que este grupo de leyes, pese a ser el que peor performa en 6 de los 7 índices, es el que tiene, en promedio, más instrumentos. Los instrumentos fueron incluidos al análisis porque representan, tal como se explicó en la sección *¿Cómo se protegen los datos personales?*, una manera de exigir el correcto cumplimiento de los derechos de los titulares. De esta forma, el hallazgo es relevante a los fines del presente estudio, e

invita a pensar qué implica una buena ley de datos personales. Con esto no quiero decir que estas leyes estén mal categorizadas como "Leyes con baja protección": aun cuando brindan a los titulares numerosos instrumentos, no reconocen derechos básicos. En suma, algunas ni siquiera designan o crean una autoridad de aplicación (Paraguay y República Dominicana).

Otro punto que destaca es que la baja protección que brindan estas leyes no es resultado (al menos para la mayoría de los casos) de que las leyes de estos países hayan sido sancionadas hace mucho tiempo. Cuba sancionó su ley de protección de datos en 2023 y es, al momento de la escritura del presente, la última ley en haber sido sancionada en la región. A su vez, Antigua y Barbuda y República Dominicana sancionaron sus leyes de protección de datos personales en 2013.

Leyes con buena protección de derechos digitales

El conjunto de leyes con buena protección de derechos digitales está compuesto por Argentina, Colombia, Costa Rica, México, Nicaragua, Panamá, Perú, Saint Kitts y Nevis y Uruguay. Fue difícil encontrar un nombre adecuado para este clúster, debido a que las leyes que lo componen no fueron las que mejor desempeñaron para ninguna de las características estudiadas. De hecho, el clúster compuesto por Barbados y Ecuador, aquel que nombramos Leyes abarcativas, reconoce numerosos derechos que el clúster en cuestión no contempla. En su mayoría, estos derechos reconocidos en las Leyes abarcativas refieren en su mayoría a derechos que fueron incorporados al marco normativo europeo con GDPR, tales como el derecho a no ser sujeto a decisiones automatizadas, el derecho a la portabilidad, y numerosos derechos a ser informado respecto de características del tratamiento a la hora de brindar consentimiento.

Sin embargo, se decidió por llamar a este grupo "Leyes con buena protección de derechos digitales" debido a que, como se explica en secciones posteriores, se consideró que los análisis más interesantes que pueden hacerse respecto de los resultados análisis de clústers emergen de la comparación entre este grupo de leyes y las que llamamos "Leyes con autoridades robustas". Y sucede que este grupo de Leyes con buena protección de derechos digitales reconoce una mayor

cantidad de beneficios, derechos y prerrogativas a los titulares por sobre sus datos personales, si se lo compara con el clúster de Leyes con autoridades robustas. Este punto permitirá desarrollar más adelante un argumento en torno a qué es lo que entendemos por buena protección de datos.

Cabe destacar que, considerando que se argumentará que Ecuador y Barbados incorporaron en gran medida el modelo de ley de protección de datos propuesto por GDPR, el grupo de Leyes con buena protección de derechos digitales es el grupo con un "diseño local" con más derechos reconocidos (en promedio). En este sentido, sería interesante entender el éxito relativo de este tipo de diseños legales. Aportar evidencia a la viabilidad de modelos legales diferentes al propuesto por GDPR debe ser uno de los pilares de la evolución de la protección de datos personales, para así romper con lógicas poscoloniales como el Efecto Bruselas, los cuales alejan las tomas de decisiones reales de los parlamentos de la región.

Leyes con autoridades robustas

Descubrir la existencia del grupo de Leyes con autoridades robustas fue otro de los descubrimientos del estudio: no estaba contemplada la existencia de un grupo que, a pesar de no haber incorporado todos los instrumentos de GDPR al pie de la letra, lograse autoridades más robustas que aquellos países que si (Ecuador y Barbados).

El grupo de leyes con autoridades robustas se caracteriza, como su nombre lo indica, por haber desempeñado mejor que todo el resto de los clústers en el índice en cuestión. El mismo, cabe recordar, se compone de variables destinadas a medir la institucionalidad de las autoridades, sus poderes informativos y coercitivos, y su participación en procesos de formulación de leyes.

Al igual que el clúster de Leyes con buena protección de derechos digitales, este grupo de leyes con autoridades robustas invita a evaluar la manera en la cual se formulan estas leyes en la región: tanto la ley de Bahamas como la de Santa Lucía son anteriores a GDPR. Si bien es cierto que el llamado Efecto Bruselas no comenzó con la Regulación General de Datos Personales, sino que se

remonta a 1985, queda claro que Latinoamérica y el Caribe no esperaron a la publicación de GDPR para sancionar leyes con atributos destacables.

Leyes abarcativas

Este último grupo de leyes, compuesto por las leyes de protección de datos personales de Ecuador y Barbados, es el que mejor desempeñó para seis de los siete índices medidos. En suma, subrayamos el hecho de que son a su vez las únicas dos leyes que incorporaron elementos muy innovadores de GDPR, tales como la exigencia a los responsables y encargados de designar delegados de protección de datos (DPOs), o realizar las evaluaciones de impacto al llevar a cabo tratamientos a gran escala o espacios públicos (Saint Kitts y Nevis, Brasil y México también, pero solamente contemplan su existencia y no se lo exigen a los responsables).

Al analizar cuán alta es la protección que ofrecen estas leyes, es menester recordar que las variables fueron diseñadas en función del articulado de GDPR. En este sentido es lógico que, si dos países emularon la regulación europea, los mismos presenten un alto índice de protección. Sin embargo, estos casos invitan a la reflexión y al debate: ¿alcanza con sancionar una ley considerablemente similar a GDPR para argumentar que existe una "buena protección de datos"? El hecho de que el presente estudio haya sido enfocado en los aspectos "de iure" de la protección de datos plantea una limitación, o al menos no brinda las mejores herramientas, a la hora de responder esta pregunta. Tal como se discutirá en mayor profundidad en la sección de *Conclusiones*, los Estados de Latinoamérica y el Caribe son diferentes a los de Europa, y es crucial considerar hasta qué punto es eficiente la estrategia adoptada por Ecuador y Barbados.

El estudio de las estadísticas descriptivas comparadas de los clústers revela diferencias significativas entre los valores de las medianas de cada índice para cada clúster. En particular, el clúster de Leyes con una baja protección de datos personales y el de Leyes abarcativas representan los grupos que tienen leyes con menor y mayor grado de protección, respectivamente. Mientras que el clúster de Leyes con una baja protección de datos personales se encuentra entre los clústers

con peores desempeños para seis de los siete índices utilizados, el clúster de Leyes abarcativas desempeña entre los mejores resultados para seis de los siete índices utilizados.

En los siguientes párrafos se hará especial hincapié en las comparaciones entre el clúster de Leyes con una alta protección de derechos digitales y el clúster de Leyes con autoridades de aplicación robustas.

¿Con qué criterios comparamos las leyes de protección de datos de América Latina?

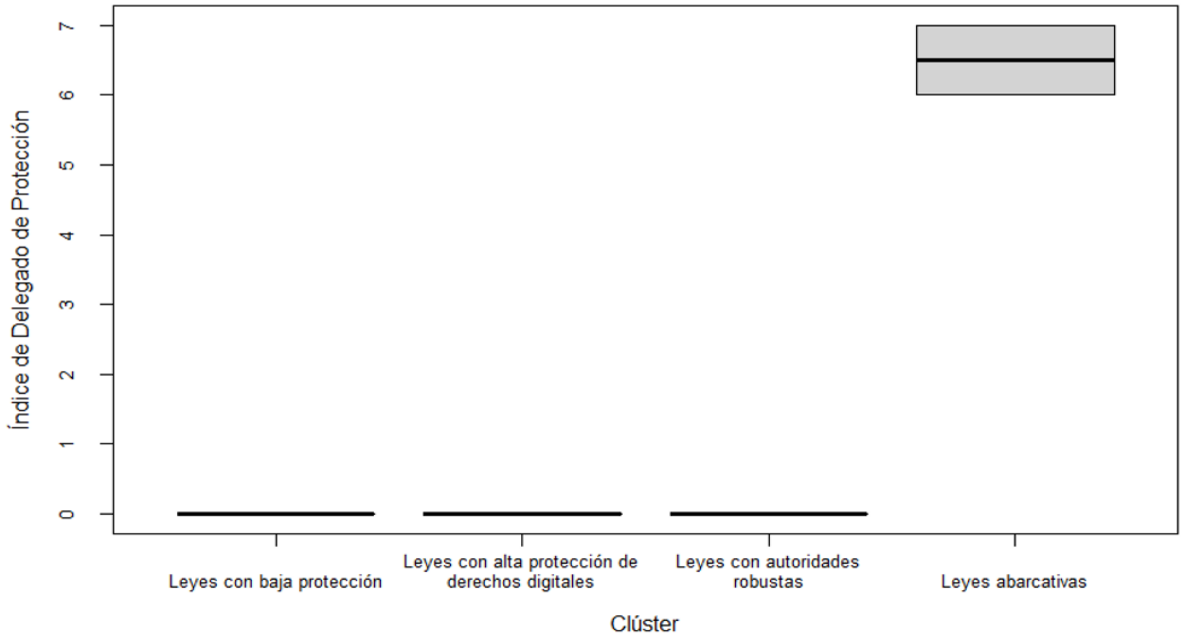
Para la comparación de las medianas de los índices para cada clúster se utilizaron boxplots[51], para así poder obtener, además, información sobre el rango intercuartil, el rango, el grado de dispersión y la presencia de posibles outliers.

[51] Un boxplot es un gráfico que muestra la mediana y la dispersión de un conjunto de datos. La caja representa el rango intercuartílico y los bigotes indican los valores atípicos. Es útil para visualizar la distribución de los datos de manera sencilla.

Delegado de protección de datos personales

Figura 3

Comparación de resultados del Índice de Delegado de Protección según clúster



El índice DPO[52] fue incluido para representar aquellas características de GDPR que se encontraban presentes solo en Ecuador y Barbados. Estas características no eran solo la existencia de un delegado de protección de datos (*data protection officer*), sino que eran múltiples los índices que tenían valores distintos de cero solo para Ecuador y Barbados. Se optó por incluir uno de estos índices por diversos motivos. En primer lugar, Ecuador y Barbados tienen leyes únicas para la región, y no incluir este índice hubiese resultado en una gran pérdida de su singularidad. En segundo lugar, muchos de los índices atendían a variables latentes de gran interés para el estudio: la existencia o ausencia de un Data Protection Officer fue desde el comienzo del estudio uno de

[52] Delegado de protección de datos, ver sección *¿Cómo se protegen los datos personales?*

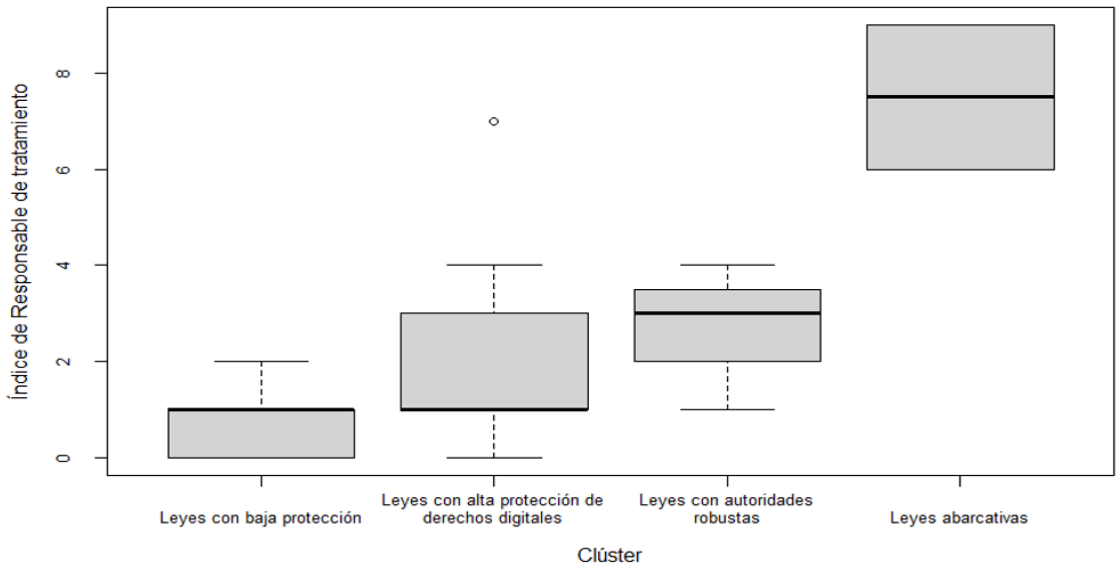
los puntos de interés teórico, y no se hubiese podido dar con una imagen de la protección de datos en América Latina y el Caribe tan nítida de no haber sido incluido el índice en el estudio.

Como se ha dicho anteriormente, las estadísticas descriptivas por clúster del índice DPO[53] reflejan un factor importante de la protección de datos en la región: solo Ecuador y Barbados son los países que cuentan con leyes que han adoptado los instrumentos de protección de datos más innovadores presentes en GDPR.

Responsables y encargados de tratamiento

Figura 4

Comparación de resultados del Índice de Responsable de Tratamiento según clúster



El índice de Responsable de Tratamiento aglutina las variables que estudian la existencia de figuras como la del responsable de tratamiento, encargado de tratamiento y representante del responsable.

[53] En figura 3.

a su vez, también incluye variables que analizan las responsabilidades que la ley asigna a estas figuras.

La comparación de las medianas de cada clúster para el índice DPO[54] muestra que es nuevamente el clúster de países con leyes abarcativas el que se destaca ampliamente por sobre el resto. A su vez, el clúster de Leyes con una baja protección de datos personales exhibe los peores resultados para este índice. Cabe destacar que este último clúster contiene incluso países para los cuales este índice vale cero. Dicho valor para esta variable implica que las leyes de dichas unidades de análisis no regulan ni contempla la existencia de responsables de tratamiento de datos personales, ni de los encargados. Esto tiene serias implicancias dado que, como se mencionó en la sección de *La protección de datos en América Latina y el Caribe*, la incorporación de la figura del responsable es fundamental dado que permite a los titulares de datos hacer valer sus derechos.

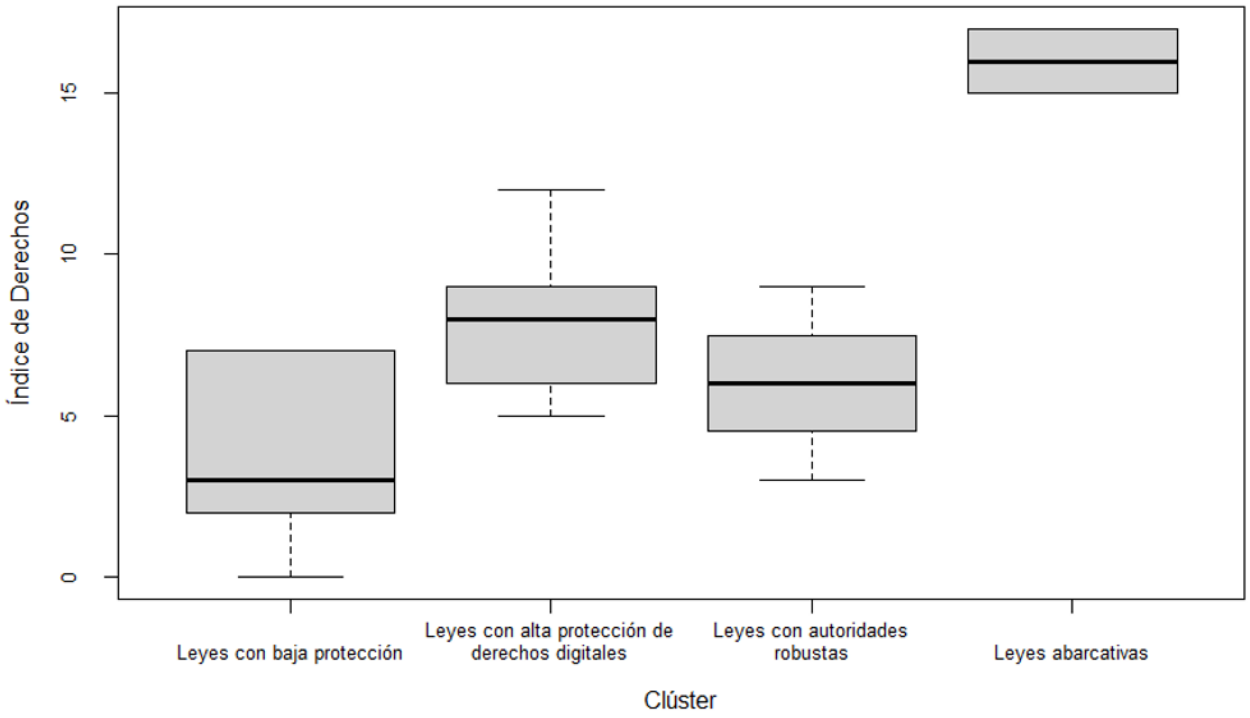
Si bien la mediana del clúster de países con Leyes con autoridades de aplicación robustas es mayor a la del clúster de Leyes con una alta protección de derechos digitales, parece haber grandes diferencias entre las medias de ambos grupos.

[54] Figura 4.

Derechos

Figura 5

Comparación de resultados del Índice de Derechos según clúster



El índice de derechos es el tercer y último índice para el cual el clúster de Leyes abarcativas se destaca ampliamente por sobre el resto[55]. Si se presta atención a las mediciones de las variables que comienzan con los códigos DS_INF y DS_R, se notará rápidamente que son Ecuador y Barbados los únicos países que reconocen el derecho del titular a ser informado acerca de numerosas características del tratamiento a la hora de dar el consentimiento.

Teniendo en cuenta consideraciones realizadas en la sección donde se abordó la naturaleza dual del dato, se decidió a los fines de este estudio considerar que una mayor cantidad de derechos es una forma de acortar la brecha de poder entre los responsables del tratamiento y los titulares los

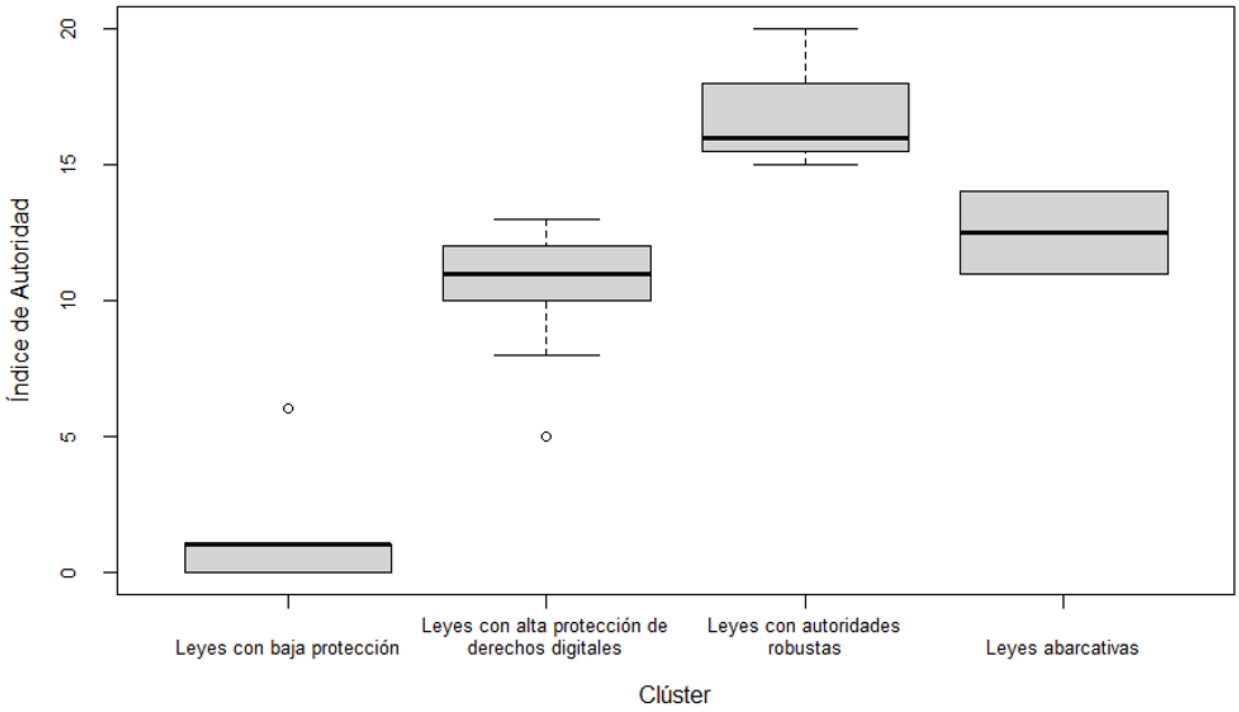
[55] Ver en Figura 5

datos, a la vez que contribuye a la construcción de un acercamiento más desmercantilizado a la protección de datos. No obstante, la existencia o el reconocimiento de numerosos derechos no significa de por sí un empoderamiento de los usuarios: hacen falta instrumentos de enforcement para asegurar el correcto acceso y cumplimiento.

Autoridad de aplicación

Figura 6

Comparación de resultados del Autoridad de Aplicación según clúster



El boxplot que refleja las estadísticas descriptivas del índice de autoridad de aplicación para cada clúster[56] revela que, tal como su nombre lo indica, el clúster de Leyes con autoridades robustas es el que más poderes, independencias, prerrogativas y obligaciones asigna a sus autoridades

[56] Figura 6.

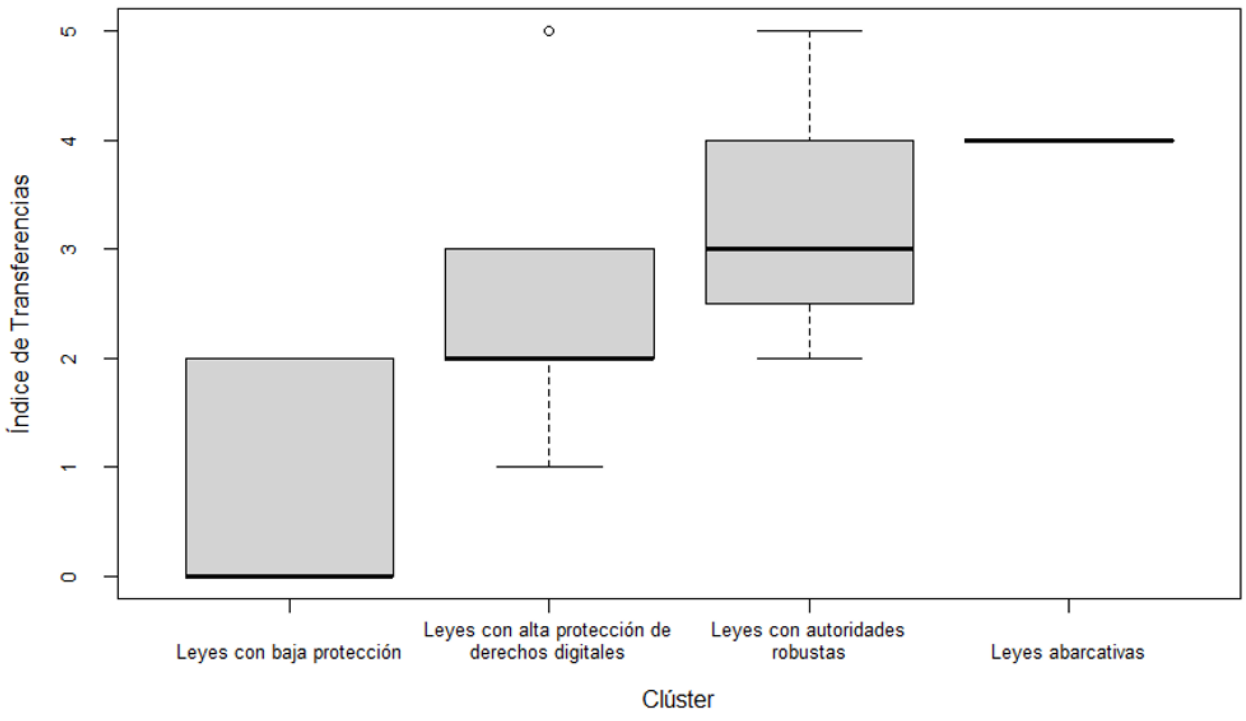
responsables de la aplicación de la ley, incluso más que las del clúster compuesto por Ecuador y Barbados.

Este. nos permite reflexionar respecto a las condiciones necesarias y suficientes para que una ley de protección de datos personales sea efectiva. Tal como se mencionó en el párrafo anterior, el reconocimiento de numerosos derechos podría no ser suficiente para garantizar el empoderamiento de los titulares de los datos.

Transferencias internacionales

Figura 7

Comparación de resultados del Transferencias Internacionales según clúster



Como se mencionó en secciones anteriores, las cláusulas que regulan la transferencia a terceros países y a organizaciones internacionales son un componente central a la hora de pensar los efectos de la regulación de datos personales en la creación y existencia de mercados de datos personales.

El boxplot analizado muestra que el clúster de Leyes abarcativas es el que cuenta con el valor más alto para el índice en cuestión. Luego, el clúster de Leyes con autoridades robustas (Brasil, Bahamas, Santa Lucía) presenta mejores resultados que los dos restantes.

Los Índices de Consentimiento y de Instrumentos no aportaron información adicional.

El impacto de GDPR en las leyes de protección de datos de América Latina y el Caribe

En la siguiente sección se aportó evidencia empírica muy sólida a favor de la hipótesis de que los países de América Latina y el Caribe han emulado GDPR. Aquellos países que sancionaron sus leyes de protección de datos personales después de la publicación de GDPR en 2016 tienen, en promedio, leyes mucho más parecidas a la regulación europea, aportando evidencia robusta a favor de la hipótesis 2. A su vez, se encontró evidencia a favor de que los países más democráticos sancionan leyes con mejor protección de datos personales.

El objetivo de este estudio fue analizar la relación entre la sanción de GDPR en 2016 y el nivel de protección de datos personales de las leyes en América Latina y el Caribe. Se recopilaron datos de las 19 observaciones para realizar el análisis. El estudio de los resultados de los 4 modelos de regresión realizados sugiere que hay una fuerte asociación entre la variable independiente de interés y el nivel de protección de datos personales de las leyes de las leyes.

Se construyeron cuatro modelos de regresión lineal[57], con el objetivo de controlar por variables intervinientes e intentar comprender mejor el impacto causal de los factores incorporados al análisis. La variable independiente de interés mide si la ley fue sancionada antes o después de 2016, y se la llamó POST_GDPR. Para construirla y medirla se optó por un nivel de medición nominal dicotómico, donde los países cuyas leyes de protección de datos personales fueron sancionadas luego del año 2016 reciben el valor "1", mientras que aquellos países con leyes anteriores a 2016 recibieron el valor "0". A su vez, se introdujeron variables al estudio con el objetivo de controlar por variables intervinientes. A esos fines, se tomaron variables de bases de datos tales como Quality of Government[58] y Varieties of Democracy[59] correspondientes a una dimensión institucional, tales como índice de democracia y tipo de régimen. A su vez, se controló por tamaño de la población en 2019. Por último, se incorporó una variable dicotómica para señalar la pertenencia del país a la Commonwealth[60]. Esto se debe a que dicha organización publicó un modelo de ley de protección de datos para sus países miembros.

El primer modelo es una regresión lineal simple, que analiza el efecto de la variable POST_GDPR en el nivel de protección de una ley. La variable es etiquetada en el cuadro como "Ley antes o después de 2016". El modelo en cuestión presenta un intercepto estadísticamente significativo al 1% (dado que su p-valor es menor a 0,01), y tiene interpretación sustantiva, ya que indica que cuando la variable independiente valga 0 (es decir, cuando la ley haya salido antes de 2016) la protección de datos personales tomará un valor esperado en promedio de 46,6. Sin embargo, lo

[57] Ver Tabla 3

[58] Teorell, Jan, Aksel Sundström, Sören Holmberg, Bo Rothstein, Natalia Alvarado Pachon, Cem Mert Dalli & Yente Meijers. 2023. The Quality of Government Standard Dataset, version Jan23. University of Gothenburg: The Quality of Government Institute, https://www.gu.se/en/quality-government doi:10.18157/qogstdjan23

[59] Coppedge, Michael, John Gerring, Carl Henrik Knutsen, Staffan I. Lindberg, Jan Teorell, David Altman, Michael Bernhard, Agnes Cornell, M. Steven Fish, Lisa Gastaldi, Haakon Gjerløw, Adam Glynn, Ana Good God, Sandra Grahn, Allen Hicken, Katrin Kinzelbach, Joshua Krusell, Kyle L. Marquardt, Kelly McMann, Valeriya Mechkova, Juraj Medzihorsky, Natalia Natsika, Anja Neundorf, Pamela Paxton, Daniel Pemstein, Josefine Pernes, Oskar Ryd´en, Johannes von R¨omer, Brigitte Seim, Rachel Sigman, Svend-Erik Skaaning, Jeffrey Staton, Aksel Sundstr¨om, Eitan Tzelgov, Yi-ting Wang, Tore Wig, Steven Wilson and Daniel Ziblatt. 2023. "V-Dem [Country-Year/Country-Date] Dataset v13" Varieties of Democracy (V-Dem) Project. https://doi.org/10.23696/vdemds23.

[60] El código utilizado en la base de datos para referir a esta variable es COMMONWEALTH

interesante del modelo uno yace en el análisis de la pendiente. La misma es estadísticamente significativa al 5% (dado que su p-valor es menor a 0,05). Esto quiere decir que se puede afirmar con suficiente evidencia que existe una asociación entre las variables, siguiendo nuestro modelo. El signo de la pendiente es positivo, lo cual indica que, al pasar de ser publicada antes de 2016 a después de dicho año, se espera en promedio que aumente el nivel de protección. Respecto a la magnitud, se espera que la protección aumente en promedio 20,2 puntos cuando un país tiene una ley sancionada después de 2016 en relación a uno cuya ley de protección de datos personales fue sancionada antes de dicho año.

El modelo 2 es una regresión lineal múltiple. Busca comprender en mayor profundidad el impacto de la variable POST_GDPR en el nivel de protección de datos de las leyes, pero controla por el impacto del índice de democracia. El índice de democracia es una variable tomada de la base de datos de Varieties of Democracy. A diferencia del modelo anterior, el intercepto no es estadísticamente significativo. El mismo cuenta con una interpretación sustantiva: en aquellos países completamente autocráticos donde la ley sea previa a 2016, se espera que, en promedio, la ley de protección de datos personales tenga un índice de protección de datos personales de 20,6 puntos. Respecto a las pendientes, la del índice de democracia es estadísticamente significativa al 1%, dado que su p-valor es menor a 0,1. Esto quiere decir que, siguiendo el modelo 2, se puede afirmar con considerable evidencia estadística que existe una asociación entre las variables. Esta asociación es positiva, dado que el coeficiente presenta signo positivo. Por lo tanto podemos esperar que, si se observan dos países cuya única diferencia es que uno es un régimen absolutamente no democrático y el otro es uno absolutamente democrático, la protección de datos personales de la ley del país democrático sea mayor que la de su hipotético gemelo. En suma, al analizar la magnitud del coeficiente correspondiente al índice de democracia, podemos afirmar con considerable evidencia estadística que se espera que el cambio en el índice de protección de datos personales mencionado sea, en promedio, de 39,9 puntos. En cuanto al impacto de la variable que estudia si la ley fue sancionada antes o después de 2016 dentro del modelo 2, la pendiente de la variable presenta una significancia estadística del 1%, dado que el p-valor es menor a 0,01. La misma tiene signo positivo, lo cual indica que se espera que en promedio aquellas leyes sancionadas post 2016 tengan mayor nivel de protección de datos personales. Por último, la

magnitud de esta pendiente es de 29,8. Esto quiere decir que al comparar un país con una ley de protección de datos personales previa a 2016 con un país que sancionó una ley con dicha competencia luego de 2016, se espera que la ley sancionada luego de 2016 tenga, en promedio, una mayor protección de datos personales a razón de casi 30 puntos. Cabe destacar que la bondad de ajuste del modelo 2 es considerablemente alta, alcanzando un valor de 0,409. Esto significa que el modelo 2 explica hasta un 40,9% de la varianza en la protección de datos personales de las leyes, utilizando tan solo dos variables.

El modelo 3 también es una regresión lineal múltiple, en la cual se incorporó la pertenencia a la Commonwealth como variable de control, y se mantuvo la variable de fecha de sanción de la ley de protección de datos en relación al año 2016 como variable independiente de interés. La variable de pertenencia a la Commonwealth se incorporó de la base de datos Quality of Government, de la versión cross-section 2019. El intercepto del modelo 3 es significante al 1%, dado que su p-valor es menor a 0.01. Esto es relevante dado que tiene una interpretación sustantiva de interés para el estudio: el modelo sugiere que se espera que el nivel de protección de una ley de protección de datos personales sancionada antes de 2016 y perteneciente a un país que no forma parte de la Commonwealth tenga, en promedio, 43,3 puntos en el índice de protección de datos de América Latina y el Caribe. Respecto a las pendientes de las variables independientes, la variable de interés presentó resultados muy similares a aquellos del modelo 1: se puede afirmar con suficiente evidencia estadística que existe una asociación entre las variables, siguiendo nuestro modelo. El signo de la pendiente es positivo, lo cual indica que, al pasar de ser publicada antes de 2016 a después de dicho año, se espera en promedio que aumente el nivel de protección. Respecto a la magnitud, se espera que la protección aumente en promedio 19,7 puntos cuando un país tiene una ley sancionada después de 2016 en relación a uno cuya ley fue sancionada antes de dicho año. La pendiente de la segunda variable si presenta resultados novedosos: la pertenencia a la Commonwealth presenta un p-valor de 0.16, por lo cual solamente es significante estadísticamente al 16%. Por ende, no hay evidencia empírica para afirmar que hay asociación sustantiva entre las variables. Sin embargo, es interesante detenerse en esta variable por un momento. La misma fue incluida en el estudio debido a que la ley modelo de la Commonwealth también fue publicada luego de 2016, y se sospechaba que no incluirla en el análisis podía devenir en una amplificación

indebida del efecto de GDPR. No obstante, al haber controlado por esta variable, podemos afirmar con mayor seguridad que en cuanto a influencia de leyes modelo refiere, GDPR no ha sido ampliamente sobreestimada. En futuros estudios podría ser relevante estudiar la influencia de otras leyes, tales como la Ley de Privacidad del Consumidor de California (CCPA).

El último modelo estudiado fue el modelo 4, el cual utiliza todas las variables incluídas en este modelo de regresión lineal múltiple: el índice de democracia, el tipo de régimen, la pertenencia a la Commonwealth, la sanción antes o después de 2016 y la población en 2019. El intercepto no tiene una interpretación sustantiva. En cuanto a las pendientes de las variables, lo único relevante es que la variable independiente de interés, “Ley antes o después de 2016”, mantuvo una significancia estadística al 10%, dado que su p-valor fue menor a 0,1. Haber hallado que esta variable no perdió su significancia estadística pese a haber incorporado otras 4 variables siguiendo criterios teóricos indica que la hipótesis de asociación entre las variables es robusta y presenta considerable evidencia empírica a su favor.

Tabla 3

Modelos de regresión lineal múltiple: ¿qué define el nivel de protección de datos de una ley?

	Dependent variable:			
	Índice de Protección de Datos Personales en América Latina y el Caribe			
	(1)	(2)	(3)	(4)
Indice de democracia		39.891*		32.173
		(19.930)		(21.432)
Régimen federal o unitario				-11.235
				(17.559)
Pertenencia a Commonwealth			13.000	47.296
			(8.901)	(29.204)
Ley antes o después de 2016	20.131**	29.776***	19.667**	23.187*
	(8.385)	(9.203)	(8.125)	(10.948)
Población 2019				5.285
				(5.744)
Constant	46.583***	20.592	43.333***	-60.295
	(5.090)	(12.852)	(5.407)	(94.468)
Observations	19	15	19	15
R^2	0.253	0.493	0.341	0.617
Adjusted R^2	0.209	0.409	0.259	0.404
Residual Std. Error	17.631 (df = 17)	16.697 (df = 12)	17.071 (df = 16)	16.771 (df = 9)
F Statistic	5.764** (df = 1; 17)	5.843** (df = 2; 12)	4.141** (df = 2; 16)	2.896* (df = 5; 9)
Note:				*p<0.1; **p<0.05; ***p<0.01

Conclusiones

Por medio del estudio de la Regulación General de Datos Personales (GDPR) y de las 19 leyes de protección de datos personales que han sido sancionadas en América Latina y el Caribe , se logró confeccionar un amplio cuadro metodológico para el estudio del nivel de protección de datos en la región, incorporando por primera vez métodos cuantitativos al estudio de esta temática en la región.

Se confeccionó el Índice de Protección de Datos Personales de América Latina y el Caribe, y se formularon 160 variables y 7 índices que podrán ser utilizados en futuras investigaciones. Con la confección de este índice se espera no sólo contribuir a la literatura académica en torno a la protección de datos personales en la región: pretendemos proponer un marco metodológico para seguir analizando y actualizando los marcos normativos en América Latina y el Caribe. Creemos que el Índice de Protección de Datos Personales en América Latina y el Caribe puede ser un buen instrumento para que la academia y las organizaciones de la sociedad civil que trabajan en torno a derechos digitales puedan realizar tareas de *assessment* constante del estado de la protección de datos en la región.

Se aportó evidencia significativa a favor de la hipótesis de que los países de América Latina están emulando fielmente al marco normativo europeo, por medio del diseño de un modelo de regresión lineal múltiple. A su vez, se encontró evidencia que sugiere que los países más democráticos sancionan leyes con un nivel de protección de datos mayor.

Se logró identificar cuatro grupos bien definidos de leyes en la región: uno con una baja protección de datos personales, uno con una alta protección de derechos digitales, un tercer grupo con autoridades de aplicación muy robustas y, por último, un grupo de países con leyes muy abarcativas

Antes de finalizar me gustaría realizar una serie de consideraciones. En particular, me gustaría detenerme en el hallazgo de que los países de la región efectivamente han emulado GDPR. Tras casi cinco años de implementación, es claro que la ley y su aplicación tienen algunos aspectos que podrían ser mejorados. Sin embargo, me parece crucial que los países de Latinoamérica y el Caribe estén actualizando sus marcos normativos, y elevando notablemente el nivel de protección de sus leyes de datos personales. Sin perjuicio de lo anterior, creo que es menester evaluar algunos aspectos de este proceso de emulación del marco normativo europeo en la región.

En primer lugar, existen algunas diferencias entre los estados de la Unión Europea y los Estados de Latinoamérica y el Caribe que requieren ser escrutados con detenimiento. El primero de ellos es que la Regulación General de Datos Personales es, como su nombre lo indica, una regulación sancionada en el marco del sistema legal de la Unión Europea, y no una ley sancionada en un parlamento de uno de sus países. Es por eso que la ley no contiene algunos de los elementos propios de una ley nacional, dado que cada uno de los países de la Unión Europea ha reglamentado GDPR en su propio marco jurídico, detallando y operacionalizando gran parte de las cláusulas. En este sentido, incorporar acríticamente a los marcos legales de nuestra región un modelo de ley que no fue diseñado para un sistema jurídico de las mismas características, dimensiones ni formas de organización tiene sus problemas. Uno de ellos, y el que más me preocupa, es que GDPR presenta pocas exigencias al Estado, dado que esa suele ser una dimensión que se regula a nivel nacional. Incorporar los elementos, o incluso el articulado textual, de GDPR puede devenir, por ende, en una ley de protección con escasas responsabilidades, obligaciones, límites ni frenos al Estado. En este sentido, me parece crucial emprender nuevas líneas de investigación que busquen identificar estas incompatibilidades.

Una de las constantes en la producción intelectual de la región desde el inicio de la construcción de los estados modernos ha sido la comparación con las leyes europeas. Intelectuales como Alberdi planteaban la necesidad de construir instituciones y marcos legales sin atender a las configuraciones europeas. La crítica a la emulación de las leyes del viejo continente partía de la base de que las realidades que atraviesan a cada una de sus sociedades son diferentes. De ahí que la propuesta de estos intelectuales era la formulación de instituciones propias, que atendieran de manera realista al contexto de la región. Varios siglos después, ese debate sigue estando vigente, y ante resultados como el que se ha hallado es menester analizar si tiene sentido incorporar a las leyes de la región todos los derechos reconocidos por GDPR cuando las instituciones no son las mismas. Creo necesario seguir ahondando en el estudio del impacto de los cambios en los marcos normativos extranjeros en aquellos de la región de América Latina, enfocándose también en la protección de datos personales *de facto*.

En segundo lugar está la diferencia de tipo de gobierno: los estados europeos son en su mayoría parlamentarios o semi-presidenciales, mientras que los países de América Latina y el Caribe son en su amplia mayoría presidencialistas. En este sentido, en América Latina y el Caribe se desarrolla lo que la literatura llama legitimidad dual[61]: tanto el presidente como el Poder Legislativo son electos por voto democrático, y por tanto ambos pueden percibirse como la encarnación de la voluntad popular. Esta característica hace que la dinámica de relación entre el Poder Ejecutivo y el Legislativo sea eminentemente diferente en los presidencialismos: funciona como un sistema de frenos y contrapesos entre los poderes del Estado[62]. La idea de frenos y contrapesos, presentada en la obra de Hamilton, Madison y Jay, es una de las bases teóricas de la república moderna. Siguiendo esta línea, al emular GDPR los Poderes Legislativos de América Latina y el Caribe podrían estar pasando por alto la inclusión de los suficientes mecanismos de control al Ejecutivo. Esta falencia horadaría la posición relativa de los Poderes Legislativos de América Latina y el Caribe frente a los Ejecutivos.

Me gustaría detenerme en las diferencias entre el grupo de leyes con alta protección de derechos digitales y el grupo de leyes con autoridades robustas. Como se explicó en la sección *¿Con qué criterios comparamos las leyes de protección de datos personales en América Latina y el Caribe?*, estos clústers de leyes presentan dos diferencias fundamentales: mientras uno tenía, en promedio, más cantidad de derechos reconocidos, el otro tenía autoridades mucho más robustas, independientes y con amplios poderes de *enforcement*. Tuve la oportunidad de exponer mis hallazgos a Gaspar Pisanu, Policy & Advocacy Manager de Access Now para Latinoamérica, con quien discutimos estas diferencias. Él sostuvo que, en su experiencia, siempre es mejor tener autoridades muy robustas, debido a que es lo que favorece el correcto cumplimiento de la ley. Tener leyes con una gran amplitud de derechos cubiertos pero sin una autoridad de aplicación que exija y presione a los responsables y encargados puede devenir en una protección *de facto* muy

[61] Mainwaring, S., & Shugart, M. S. (1994). Juan J. Linz: Presidencialismo y democracia. Una revisión crítica. *Desarrollo Economico-revista De Ciencias Sociales*, *34*(135), 397. https://doi.org/10.2307/3467274

[62] Hamilton, A., Madison, J., & Jay, J. (1875). *The Federalist: A Commentary on the Constitution of the United States. A Collection of Essays*.

distinta a aquella escrita en la ley. Pisanu también señaló que es menester recordar que la prioridad debe estar en seguir subiendo los estándares de protección en la región.

También tuve la oportunidad de dialogar sobre la protección de datos personales en la región con Agustín Frizzera, Director Ejecutivo de Democracia en Red. Respecto de la necesidad de seguir mejorando el estándar de protección de datos personales en América Latina, Agustín resaltó la importancia de la instauración de procesos obligatorios para informar a los titulares y a las autoridades respecto de vulnerabilidades en la seguridad de los datos personales. También destacó la necesidad de garantizar la independencia de las autoridades de aplicación, y la inclusión del derecho a no ser sujeto de decisiones automatizadas.

Mi objetivo al conversar con Agustín Frizzera y Gaspar Pisanu era comprender mejor la visión que tienen los actores de la sociedad civil respecto a la protección de datos personales y los procesos de formulación de las leyes. Ambos trabajaron intensamente en instancias participativas con el objetivo de incidir en las leyes de protección de datos personales. Me gustaría destacar la importancia de la participación de la sociedad civil en espacios legislativos donde se escriben estas leyes. Al conversar con Agustín y Gaspar, ambos señalaron que la temática de protección de datos personales requiere un nivel de *expertise* técnico elevado, y muchas veces los legisladores no tienen las herramientas para devenir con una ley a la altura de las circunstancias. En este sentido, ambos subrayaron la necesidad de fortalecer los espacios de participación de la sociedad civil, la academia y del sector técnico. A su vez, destacamos la importancia de la articulación entre estos actores para la confección de herramientas que asistan a los poderes legislativos en la toma de decisiones en torno a la protección de los datos personales.

Subrayamos la importancia de emprender nuevas investigaciones en torno a la regulación de datos personales en América Latina y el Caribe. Comprender las tendencias de iure y los impactos en la práctica permiten asegurar el correcto cumplimiento de los derechos digitales en el contexto de la Era de la Información. En este sentido, sugerimos incorporar la utilización de instrumentos cuantitativos para el estudio de la temática.

Bibliografía

Bradford, A. (2020). "The Brussels Effect: How the European Union Rules the World". Oxford University Press.

Brown, I. (2013). "Research Handbook on Governance of the Internet". Edward Elgar Publishing.

Carrillo, A. J., & Jackson, M. (2022). "Follow the Leader? A Comparative Law Study of the EU's General Data Protection Regulation's Impact in Latin America". *ICL online journal*, *16*(2), 177-262.

Convention 108+. (2008, junio). Council of Europe. Recuperado 10 de julio de 2023.

Greenleaf, G. (2012). "The influence of European Data Privacy Standards outside Europe: Implications for Globalization of Convention 108". *International Data Privacy Law*, *2*(2), 68-92.

Hair, J., Anderson, R., Black, B., & Babin, B. (2016). "Multivariate Data Analysis". Pearson Higher Ed.

Hamilton, A., Madison, J., & Jay, J. (1875). "The Federalist: A Commentary on the Constitution of the United States". *A Collection of Essays*.

Kitchin, R. (2014). "The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences". *SAGE.*

Mainwaring, S., & Shugart, M. S. (1994). "Juan J. Linz: Presidencialismo y Democracia. Una Revisión Crítica". *Desarrollo Economico-revista De Ciencias Sociales*, *34*(135), 397.

Mikołajska, A. (2015). "Viktor Mayer-Schönberger, Kenneth Cukier, BIG DATA: rewolucja, która zmieni nasze myślenie, pracę i życie, przeł." M. Głatki, Warszawa: MT Biznes 2014, s. 280. *Biblioteka*, *19(28)*, 267.

Murray, A. M. (2019). "Data as a Commodity vs Data as a Right". *Policy paper, LSE*.

OPOCE. (1995). *Directiva 95/45 EC*. Recuperado 10 de julio de 2023.

Schwartz, P. M. (2019). "Global Data Privacy: The EU Way". *Publisher.*

UNIVERSIDAD TORCUATO DI TELLA

ANEXO I: "Codebook de variables para el análisis cuantitativo de las leyes de protección de datos personales de América Latina y el Caribe"

ÍNDICE

Nota del autor: 55
Fecha 55
LYEAR 55
POST_GDPR 55
Ámbito de aplicación material 55
MAT_AP 55
TRTMT_SCOPE 56
TRTMT_EXC_PERS 56
TRTMT_EXC_GOV 56
Ámbito territorial: 57
TERR_AP 57
TRTMT_TERR1 57
TRTMT_TERR2 57
TRTMT_TERR3 58
Principios 58
TRTMT_PRINC1 58
TRTMT_PRINC2 58
TRTMT_PRINC3 59
TRTMT_PRINC4 59
TRTMT_PRINC5 59
TRTMT_PRINC6 59
TRTMT_PRINC7 60
Licitud del tratamiento 60
LEGALITY_DEF 60
LEGALITY_CONS 60
Consentimiento 60
CONSENT_EASE 60
CONSENT_WD 61
CONSENT_AGE 61
Categorías especiales 61
SP_CATEGORIES_LIMIT 61

SP_CATEGORIES_EXIST 61
SP_CATEGORIES_EXC 62
PENITENTIARY_DATA 62
DATAHOLDER_ID 62
DERECHOS DEL INTERESADO 63
DS_GRATUITY 63
DC_CHARGE 63
AUTH_FEE 63
Información y acceso - Derechos del interesado: 63
TRANSPARENT_INFO 63
DS_INF_DATA 64
DS_INF_OTHER 64
DS_INF_ADD 64
DS_INF_RPD 64
DS_INF_RESP 64
DS_INF_DEL 65
DS_INF_TRTMT 65
DS_INF_OBJ 65
DS_INF_DES 65
DS_INF_TRANSF 65
DS_INF_TERM 66
DS_INF_AUTO 66
DS_INF_ALT 66
DS_INF_RIGHTS 66
DS_INF_RECTIF 66
DS_INF_CONSWD 67
DS_INF_RECL 67
Tratamiento - Derechos del interesado 67
DS_R_TRTMT 67
DS_R_PROCESS 67
DS_R_OBJ 68
DS_R_DES 68
DS_R_TERM 68
DS_R_ORIGIN 68
DS_R_AUTO 69
DS_R_ADEQUACY 69
DS_R_COPY 69
DS_R_AUTH 69
DS_R_SUPR 70
DS_R_OPO 70
DS_R_OPO1 70

DS_R_OPO2 ... 70
DS_R_RECT ... 71
DS_R_SUPR_PUBLIC ... 71
Reclamos - Derechos del interesado ... 71
DS_R_ADMIN ... 71
DS_R_COMPLAINT ... 72
DS_R_JUDICIAL ... 72
DS_R_REMEDYAUTH ... 72
DS_R_REMEDYAUTH2 ... 72
DS_R_REMEDYCONTROLLER ... 73
DS_R_REMEDYCONTROLLER2 ... 73
DS_R_REPRESENTANT ... 73
DS_R_COMPENSATION ... 73
Responsable del tratamiento y encargado del tratamiento ... 74
DC_EXIST ... 74
DC_SECURITY ... 74
CO_RESPONSIBLE ... 74
REPRESENTATIVE ... 74
Encargado ... 75
PROCESSOR ... 75
PROCESSOR_CONTRACT ... 75
PROCESSOR_OTHER ... 75
PROCESSOR_ASSURANCES ... 76
TRTMT_REGISTER ... 76
Empresas pequeñas (Small business - SB) ... 76
SMALL_BUSSINESS ... 76
SB_REGISTER_EXC ... 76
Seguridad de los datos personales ... 77
Violación de seguridad - Seguridad ... 77
BREACH_AUT ... 77
BREACH_DS ... 77
Evaluación de impacto (Impact assesment - I_ASSESMENT) ... 77
I_ASSESMENT ... 77
I_ASSESMENT_A ... 78
I_ASSESMENT_S ... 78
I_ASSESMENT_P ... 78
I_ASSESMENT_AUT ... 78
P_CONSULTATION ... 79
P_ADVICE ... 79
Delegado (DPO_) ... 79
DPO_EXIST ... 79

DPO_IND 79
DPO_DESIGNATION_COMP 80
DPO_DESIGNATION_SCALE 80
DPO_DESIGNATION_SPCAT 80
DPO_CONTACT 80
DPO_TASKS 81
Códigos de conducta (CODES) 81
CODE_EXIST 81
CODE_S 81
Certificación () 82
CERTIFICATION 82
CERTIFICATION_BODY 82
Transferencia de datos personales a terceros países u organizaciones internacionales 82
TRANSF_EXIST 82
TRANSF_ADEQUACY 82
ADEQUACY_ROL 83
ADEQUACY_HR 83
ADEQUACY_DPL 83
ADEQUACY_AUTH 83
ADEQUACY_TREATIES 84
INT_COOP 84
Normas corporativas 84
BIND_C_RULES 84
Autoridades de control independientes 85
AUTH_EXIST 85
AUTH_MULTI 85
AUTH_HIERARCHY 85
AUTH_IND 85
AUTH_HIRE 86
AUTH_BUDGET 86
AUTH_DES 86
AUTH_MANDATE 86
AUTH_RENEW 86
AUTH_REGISTER 87
AUTH_COMP 87
AUTH_GOV 87
AUTH_JUDICIARY 87
AUTH_REC 88
AUTH_IP_ORDER 88
AUTH_IP_AUDIT 88
AUTH_IP_CERT 88

AUTH_IP_NOTIF 89
AUTH_IP_ACCESSD 89
AUTH_IP_ACCESSE 89
AUTH_CP_WARN 89
AUTH_CP_REPR 90
AUTH_CP_REQ 90
AUTH_CP_COMPLY 90
AUTH_CP_COMM 90
AUTH_CP_BAN 91
AUTH_CP_ERASE 91
AUTH_CP_WDW 91
AUTH_CP_AFINE 91
AUTH_CP_EXPORT 91
AUTH_AAP_ADV 92
AUTH_AAP_LEG 92
AUTH_AAP_ISSUE1 92
AUTH_AAP_ISSUE2 92
AUTH_AAP_ISSUE3 93
AUTH_JUDICIAL 93
Conciliación 93
FREESPEECH_EXIST 93
FREESPEECH_EXCEPT 93
ID_EXIST 94
WORKPLACE_EXIST 94
REPEAL 94
TREATIES 94
Otras 95
CRIMINAL_CONS 95
ECONOMIC_CONS 95
FINES_AUTH 95
AUTH_CP_AFINE 95
FED_UNI 95
COMMONWEALTH 96
Variables tomadas de bases de datos: 96
Variables tomadas de la base de datos V-Dem 96
LIBDEM 96
- Título en base original: Liberal democracy index (D) (v2x_libdem) 96
Variables tomadas de la base de datos Quality of Government 97
POP2019 97

Nota del autor:

Las variables contenidas en el presente fueron diseñadas a partir del texto de la Regulación General de Datos Personales ("GDPR", por sus siglas en inglés). El criterio utilizado para todas las variables comprendidas dicotómicas de producción propia es que el valor "1" indica "Si", mientras que el "0" significa "No", a menos que se indique lo contrario. A su vez, los enunciados de las variables fueron construidos de forma en que 1 siempre es más protección que 0, excepto para la variable POST_GDPR. Si bien no todas las variables que se encuentran a continuación fueron utilizadas en los métodos estadísticos, todas fueron medidas en las 19 leyes analizadas.

D=Dicotómica

N=Nominal

O=Ordinal

Fecha

LYEAR
- Informa el año en el que se sancionó la ley
- O
- GDPR: 2016

POST_GDPR
- La ley fue sancionada luego de la publicación de GDPR, es decir luego del 4 de mayo de 2016?
- D

Ámbito de aplicación material

MAT_AP
- La ley define el ámbito de aplicación material
- D
- GDPR:1
- GDPR_art: 2.1

TRTMT_SCOPE

- La **ley aplica para tratamiento automatizado, semiautomatizado y no automatizado** de datos
- D
- GDPR: 1
- GDPR_art: 2.1

TRTMT_EXC_PERS

- La ley no gobierna sobre el tratamiento si el mismo es efectuado por una persona física en el ejercicio de **actividades exclusivamente personales o domésticas**;
- D
- GDPR: 1
- GDPR_art: 2.2.C

TRTMT_EXC_GOV

- La ley no gobierna sobre el tratamiento si el mismo es efectuado por parte de las **autoridades competentes con fines de prevención,** investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.
- D
- GDPR: 1
- GDPR_art: 2.2.d

Ámbito territorial:

TERR_AP

- La ley define el ámbito de aplicación territorial
- D
- GDPR:1
- GDPR_art: 2.1

TRTMT_TERR1

- La ley se aplica al tratamiento de datos personales en el contexto de las **actividades de un establecimiento del responsable** o del encargado **en el país en cuestión**, independientemente de que el tratamiento tenga lugar en en el país en cuestión o no.

- D
- GDPR:1
- GDPR_art: 3.1

TRTMT_TERR2

- La ley se aplica al **tratamiento de datos personales de interesados que residan en el país por parte de un responsable o encargado no establecido en el país**, cuando las actividades de tratamiento estén relacionadas con la **oferta de bienes o servicios** a dichos interesados en el país, independientemente de si a estos se les requiere su pago
- d
- GDPR: 1
- GDPR_art:3.2.a

TRTMT_TERR3

- La ley se aplica al tratamiento de datos personales de **interesados que residan en el país por parte de un responsable o encargado no establecido en el país**, cuando las actividades de tratamiento estén relacionadas con el control de su comportamiento, en la medida en que este tenga lugar en la Unión
- D
- GDPR: 1
- GDPR_art: 3.2.b

Principios

TRTMT_PRINC1

- La ley estipula que los datos deben ser tratados de manera lícita, leal y transparente **(«licitud, lealtad y transparencia»)**
- D
- GDPR: 1
- GDPR_art: 5.1.a

TRTMT_PRINC2

- La ley estipula que los datos serán recogidos con fines determinados, explícitos, legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines. **(«limitación de la finalidad»)**

- D
- GDPR: 1
- GDPR_art: 5.1.b

TRTMT_PRINC3
- La ley estipula que los datos serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados **(«minimización de datos»).**
- D
- GDPR: 1
- GDPR_art: 5.1.c

TRTMT_PRINC4
- La ley estipula que los datos serán a exactos y, si fuera necesario, actualizados **(«exactitud»)**
- D
- GDPR: 1
- GDPR_art: 5.1.d

TRTMT_PRINC5
- La ley estipula que los datos serán mantenidos durante no más tiempo del necesario para los fines del tratamiento de los datos personales. **(«limitación del plazo de conservación»)**
- D
- GDPR: 1
- GDPR_art: 5.1.e

TRTMT_PRINC6
- La ley estipula que los datos serán tratados de forma que se garantice su seguridad y se prevenga su pérdida **(«integridad y confidencialidad»)**
- D
- GDPR: 1
- GDPR_art: 5.1.f

TRTMT_PRINC7
- La ley estipula que **responsabilidad proactiva** por parte del responsable (será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo)
- D
- GDPR: 1

- GDPR_art: 5.2

Licitud del tratamiento

LEGALITY_DEF

- La ley estipula condiciones para que el tratamiento sea lícito, haciendo que el mismo **NO sea lícito por default**
- D
- GDPR: 1
- GDPR_art: 6

LEGALITY_CONS

- Una de las condiciones para que el tratamiento sea lícito es que el interesado haya dado su **consentimiento para el tratamiento** de sus datos personales para uno o varios fines específicos
- D
- GDPR: 1
- GDPR_art: 6.1.a

Consentimiento

CONSENT_EASE

- Determina que el contexto en el que el interesado brinda **consentimiento** para el tratamiento de sus datos personales debe presentar **lenguaje claro y ser de fácil acceso**
- D
- GDPR: 1
- GDPR_art: 7

CONSENT_WD

- La ley determina que será **tan fácil retirar el consentimiento como darlo**
- D
- GDPR: 1
- GDPR_art: 7.3

CONSENT_AGE

- El consentimiento solo puede ser brindado po**r mayores de una determinada edad,** y el consentimiento de menores solo puede ser brindado por los titulares de la patria potestad o tutela sobre el niño
- D
- GDPR: 1

- GDPR_art: 8

Categorías especiales

SP_CATEGORIES_LIMIT
- El tratamiento de categorías especiales es ilícito por default, sin perjuicio de las excepciones que haya a esa condición legal
- D
- GDPR: 1

SP_CATEGORIES_EXIST
- La ley prohíbe el tratamiento de **datos que revelen** datos sensibles, termino que puede incluir (la lista es enunciativa):
    - el orígen étnico o racial
    - opiniones políticas,
    - convicciones religiosas o filosóficas
    - afiliación sindical
    - tratamiento de datos genéticos
    - trat de datos biométricos dirigidos a identificar de manera unívoca a una persona física
    - datos relativos a la salud
    - datos relativos a la vida sexual
    - orientación sexual
- D
- GDPR: 1
- GDPR_art: 9

SP_CATEGORIES_EXC
- **Existen excepciones a la prohibición de tratamiento de categorías especiales**
- D
- GDPR: 1
- GDPR_art: 9

PENITENTIARY_DATA
- La ley determina que el **tratamiento de datos relativos a condenas**, infracciones o seguridad sólo puede hacerse bajo la observación del Estado.
- D
- GDPR: 1
- GDPR_art: 10

DATAHOLDER_ID
- La ley establece que, si los fines del tratamiento no requieren identificación, el **responsable del tratamiento puede obviar esfuerzos por identificar a los interesados**.
- D
- GDPR: 1
- GDPR_art: 11

DERECHOS DEL INTERESADO

DS_GRATUITY
- La ley determina que el interesado puede hacer uso de sus derechos **sin pagar por ningún proceso**?
    - D
    - GDPR:1

DC_CHARGE
- **Habilita cobro** por parte del responsable si la solicitud es infundada o repetitiva
- D
- GDPR: 1
- GDPR_art: 12

AUTH_FEE
- La ley determina que las funciones de cada autoridad de control será gratuito para el interesado y el delegado de protección de datos.

Información y acceso - Derechos del interesado:

TRANSPARENT_INFO
- El responsable debe **brindar información al interesado de forma transparente, concisa, inteligible y de fácil acceso, lenguaje claro y sencillo**
- D
- GDPR: 1
- GDPR_art: 12

DS_INF_DATA

- El interesado puede acceder a información sobre los datos personales almacenados por el responsable?
- D
- GDPR: ?

DS_INF_OTHER

- La ley determina que **si los datos del interesado se obtuvieron de una tercera fuente, y no del interesado, se le deberá brindar la misma información que la presente en las otras variables DS**

DS_INF_ADD

- La ley determina que **si los datos del interesado se obtuvieron de una tercera fuente, y no del interesado, el responsable deberá, en un plazo razonable desde la obtención de los datos personales,** comunicar al interesado la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público;

DS_INF_RPD

- El interesado puede acceder a información sobre el responsable, encargado y/o delegado que llevan a cabo el tratamiento de sus datos personales?
- D
- GDPR:1

DS_INF_RESP

- La ley determina que, en caso de ser obtenidos por vía del interesado, el responsable brindará al interesado en el momento de la obtención de los datos **la identidad y los datos de contacto del responsable y, en su caso, de su representante;**

DS_INF_DEL

- La ley determina que, en caso de ser obtenidos por vía del interesado, el responsable brindará al interesado en el momento de la obtención de los datos la **información de contacto del delegado de protección de datos**, en su caso;

DS_INF_TRTMT

- El interesado debe ser informado sobre el tratamiento de sus datos personales?
- D
- GDPR:1

DS_INF_OBJ

- La ley determina que, en caso de ser obtenidos por vía del interesado, el responsable comunicará al interesado en el momento de la obtención de los datos **los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento**;

DS_INF_DES

- La ley determina que, en caso de ser obtenidos por vía del interesado, el responsable informará al interesado en el momento de la obtención de los datos **los destinatarios o las categorías de destinatarios de los datos personale**s, en su caso;

DS_INF_TRANSF

- La ley determina que, en caso de ser obtenidos por vía del interesado, el responsable informará al interesado en el momento de la obtención de los datos, en su caso, la **intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación.**

DS_INF_TERM

- La ley determina que, en caso de ser obtenidos por vía del interesado, el responsable informará al interesado en el momento de la obtención de los datos **el plazo durante el cual se conservarán los datos personales** o, cuando no sea posible, los criterios utilizados para determinar este plazo;

DS_INF_AUTO

- La ley determina que, en caso de ser obtenidos por vía del interesado, el responsable informará al interesado en el momento de la obtención de los datos la existencia de **decisiones automatizadas, incluida la elaboración de perfiles, e información significativa sobre la lógica aplicada**, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

DS_INF_ALT

- La ley determina que, cuando **el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron,** proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente

DS_INF_RIGHTS

- El interesado debe ser informado de sus derechos a la hora de dar consentimiento para el tratamiento?

  DS_INF_RECTIF
  - La ley determina que, en caso de ser obtenidos por vía del interesado, el responsable informará al interesado en el momento de la obtención de los datos la existencia del **derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;**

  DS_INF_CONSWD
  - La ley determina que, en caso de ser obtenidos por vía del interesado, el responsable informará al interesado en el momento de la obtención de los datos la existencia del **derecho a retirar el consentimiento en cualquier momento**, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;

  DS_INF_RECL
  - La ley determina que, en caso de ser obtenidos por vía del interesado, el responsable informará al interesado en el momento de la obtención de los datos la existencia del **derecho a presentar una reclamación ante una autoridad;**

Tratamiento - Derechos del interesado

DS_R_TRTMT

- La ley determina que el interesado tiene **derecho a obtener información sobre el tratamiento de sus datos personales**
- D
- GDPR: 1
- GDPR_art: 15

  DS_R_PROCESS
  - La ley determina que el interesado tiene derecho a **saber si sus datos personales están siendo tratados.**
  - D
  - GDPR: 1
  - GDPR_art: 15

DS_R_OBJ

- La ley dispone que el interesado tiene **derecho a conocer cuáles son los fines** que persigue el responsable o encargado a la hora de tratar sus datos personales.
- D
- GDPR: 1
- GDPR_art: 15

DS_R_DES

- La ley determina que el interesado tiene **derecho a conocer quienes son los destinatarios de sus datos personales,** sean estos terceros u organizaciones internacionales.
- D
- GDPR: 1
- GDPR_art: 15

DS_R_TERM

- La ley determina que **el interesado tiene derecho a conocer los plazos previstos** de conservación de sus datos personales, y los criterios para la definición de dicho plazo.
- D
- GDPR: 1
- GDPR_art: 15

DS_R_ORIGIN

- La ley **determina que el interesado tiene derecho a conocer cualquier información disponible sobre el origen de los datos personales cuando estos no se hayan obtenido del interesado**
- D
- GDPR: 1
- GDPR_art: 15

DS_R_AUTO

- La ley determina que el interesado tiene **derecho a saber de la existencia de decisiones automatizadas, incluída la elaboración de perfiles, y conocer la lógica aplicada**
- D

- GDPR: 1
- GDPR_art: 15

DS_R_ADEQUACY
- La ley determina que el interesado tiene derecho a conocer, en caso de que sus datos personales sean transferidos a un tercer país o a una organización internacional, las garantías adecuadas relativas a la transferencia
- D
- GDPR: 1
- GDPR_art: 15

DS_R_COPY
- La ley determina que el interesado tiene derecho a recibir una copia de los datos personales objeto de tratamiento por parte del responsable de tratamiento.
- D
- GDPR: 1
- GDPR_art: 15

DS_R_AUTH
- La ley determina que el interesado tien**e derecho a presentar una reclamación ante una autoridad de control**
- D
- GDPR: 1
- GDPR_art: 15

DS_R_SUPR
- La ley determina que el interesado tiene **derecho a solicitar del responsable la supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;**
- GDPR: 1
- GDPR_art: 17

DS_R_OPO
- La ley determina que el interesado tiene **derecho a oponerse al tratamiento** de sus datos personales si es por fines públicos o intereses legítimos del responsable o encargado
- D
- GDPR: 1
- GDPR_art: 21

DS_R_OPO1

- La ley determina que el interesado tiene derecho a oponerse al tratamiento de sus datos personales si el mismo tiene como objeto la mercadotecnia directa, incluida la elaboración de perfiles
- D
- GDPR: 1
- GDPR_art: 21

DS_R_OPO2

- La ley determina que el interesado tiene derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.
- D
- GDPR: 1
- GDPR_art: 22

DS_R_RECT

- La ley determina que el interesado tiene **derecho a solicitar del responsable la rectificación de datos personales inexactos, o que se completen aquellos incompletos.**
- GDPR: 1
- GDPR_art: 16

DS_R_SUPR_PUBLIC

- La ley determina que, **cuando el responsable haya hecho públicos sus datos personales, el interesado tiene derecho a que el responsable aplique medidas razonables para hacer saber a otros responsables que estén tratando esos datos de la solicitud del interesado de supresión de cualquier enlace, copia o réplica de los mismos.**
- GDPR: 1
- GDPR_art: 17

Reclamos - Derechos del interesado

DS_R_ADMIN

- El interesado puede comenzar una acción administrativa ante el incumplimiento de la ley?

- GDPR:1
- GDPR_art: 77

DS_R_COMPLAINT
- Todo interesado tendrá derecho a presentar una reclamación ante una autoridad
- D
- GDPR: 1
- GDPR_art: 77

DS_R_JUDICIAL
- El interesado puede comenzar una acción judicial ante el incumplimiento de la ley?
- D
  GDPR:1
- GDPR_art:78

DS_R_REMEDYAUTH
- toda persona física o jurídica tendrá derecho a la tutela judicial contra una decisión jurídicamente vinculante de una autoridad de control que le concierna
- D
- GDPR: 1
- GDPR_art: 78

DS_R_REMEDYAUTH2
- toda persona física o jurídica tendrá derecho a la tutela judicial contra una autoridad de control que no dé curso a una reclamación o no informe al interesado en el plazo de tres meses.
- D
- GDPR: 1
- GDPR_art: 78

DS_R_REMEDYCONTROLLER
- todo interesado tendrá derecho a la tutela judicial efectiva cuando considere que sus derechos en virtud de la ley han sido vulnerados como consecuencia de un tratamiento de sus datos personales.
- D
- GDPR: 1
- GDPR_art: 79

DS_R_REMEDYCONTROLLER2

- Las acciones contra un responsable o encargado se ejercitan ante los tribunales del estado en donde el responsable tiene establecimiento
- D
- GDPR: 1
- GDPR_art: 79

DS_R_REPRESENTANT

- El interesado tendrá derecho a dar mandato a una entidad, organización o asociación para que presente en su nombre una reclamación, y ejerza en su nombre los derechos y el derecho a ser indemnizado
- D
- GDPR: 1
- GDPR_art: 80

DS_R_COMPENSATION

- Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos.
- D
- GDPR: 1
- GDPR_art: 82

Responsable del tratamiento y encargado del tratamiento

DC_EXIST

- La ley contempla la existencia de un responsable, entendido como una persona física o jurídica que determina, sola o en conjunto con otras personas, los fines y los medios del tratamiento de datos personales.

DC_SECURITY

- La ley determina que el responsable deberá tomar medidas técnicas y organizativas que garanticen nivel de seguridad adecuado al riesgo.
- D
- GDPR: 1
- GDPR_art: 32

CO_RESPONSIBLE

- La ley determina que, cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones. El interesado podrá ejercer sus derechos frente a cada uno de los responsables
- D
- GDPR: 1
- GDPR_art:27

REPRESENTATIVE

- La ley establece que, cuando el responsable del tratamiento no reside en el país, deberá establecer un representante en el país. El responsable atiende junto al responsable o encargado a las consultas de la autoridad de control y de los interesados
- D
- GDPR: 1
- GDPR_art:27

Encargado

PROCESSOR

- La ley determina que el responsable del tratamiento podrá recurrir a un encargado para el procesamiento de los datos siguiendo instrucciones documentadas, incluyendo transferencias.
- D
- GDPR: 1
- GDPR_art:28

PROCESSOR_CONTRACT

- La ley determina que el responsable del tratamiento podrá recurrir a un encargado con contrato de por medio
- D
- GDPR: 1
- GDPR_art:28

PROCESSOR_OTHER

- La ley determina que el encargado no recurre a otro encargado sin permiso del responsable

- D
- GDPR: 1
- GDPR_art:28

PROCESSOR_ASSURANCES
- La ley dicta que el encargado deberá tomar medidas para garantizar seguridad y confidencialidad en el tratamiento
- D
- GDPR: 1
- GDPR_art:28

TRTMT_REGISTER
- La ley dicta que responsables y encargados deberán registrar las actividades de tratamiento efectuadas bajo su responsabilidad
- D
- GDPR: 1
- GDPR_art:30

Empresas pequeñas (Small business - SB)

SMALL_BUSSINESS
- La ley contempla la existencia de empresas pequeñas, y las excluye de algún tipo de requerimiento o restricción
- D
- GDPR: 1
- GDPR_art:30

SB_REGISTER_EXC
- La ley excluye a empresas pequeñas de registrar sus actividades de tratamiento
- D
- GDPR: 1
- GDPR_art:30

Seguridad de los datos personales

Violación de seguridad - Seguridad

BREACH_AUT
- La ley determina que, ante una violación a la seguridad de los datos personales, el responsable de tratamiento deberá notificarla a la autoridad de control competente.
- D
- GDPR: 1
- GDPR_art: 33

BREACH_DS
- Ante una violación de la seguridad de los datos personales que entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable la comunicará al interesado sin dilación.
- D
- GDPR: 1
- GDPR_art:34

Evaluación de impacto (Impact assesment - I_ASSESMENT)

I_ASSESMENT
- La ley determina que, cuando es probable que un tratamiento entrañe riesgos a derechos o libertades de personas físicas, se hace evaluación de impacto de las operaciones de tratamiento. Esto comprende procesos de prevención y mitigación de riesgos.
- D
- GDPR: 1
- GDPR_art: 35

I_ASSESMENT_A
- La ley determina que aquellos tratamientos que realicen una **evaluación sistemática y exhaustiva de aspectos personales, sobre todo cuando se basan en tratamiento automatizado, deberán ser sujetos a evaluaciones de impacto**
- D
- GDPR: 1
- GDPR_art: 35

I_ASSESMENT_S
- La ley determina que aquellos tratamientos que realicen un tratamiento a **gran escala** de las categorías especiales de datos deberán ser sujetos a evaluaciones de impacto
- D
- GDPR: 1
- GDPR_art: 35

I_ASSESMENT_P
- La ley determina que aquellos tratamientos que realicen una **observación sistemática de zona de acceso pública** deberán ser sujetos a evaluaciones de impacto
- D
- GDPR: 1
- GDPR_art: 35

I_ASSESMENT_AUT
- La ley determina que la autoridad de control puede confeccionar listas de tratamientos que requieren evaluación de impacto
- D
- GDPR: 1
- GDPR_art: 35

P_CONSULTATION
- La ley determina que, cuando la evaluación de impacto revela riesgos si no se toman medidas para mitigarlo, el responsable deberá consultar con la autoridad antes de proceder al tratamiento.
- D
- GDPR: 1
- GDPR_art: 36

P_ADVICE
- La ley determina que, si la autoridad de control define que el responsable no identificó riesgos o no los mitigó, puede introducir una prórroga para asesorar al responsable y encargado por escrito.
- D
- GDPR: 1
- GDPR_art: 36

Delegado (DPO_)

DPO_EXIST
- La ley contempla la figura de un delegado de tratamiento, entendido como una persona de la nómina del responsable o quien opera bajo contrato de servicio, a quien se delegan las actividades de protección de datos.
- D
- GDPR: 1
- GDPR_art: 38

DPO_IND
- La ley determina que el delegado no puede recibir instrucciones sobre su labor, ser destituido ni sancionado.
- GDPR: 1
- GDPR_art: 38

DPO_DESIGNATION_COMP
- La ley determina que, para al menos un tipo de tratamiento, los responsables que lo lleven a cabo deberán designar un delegado obligatoriamente
- D
- GDPR: 1
- GDPR_art: 37

DPO_DESIGNATION_SCALE
- La ley determina que, cuando el tratamiento requiera observación habitual y sistemática de interesados a gran escala, los responsables que lo lleven a cabo deberán designar un delegado obligatoriamente
- D
- GDPR: 1
- GDPR_art: 37

DPO_DESIGNATION_SPCAT
- La ley determina que, cuando el responsable lleve a cabo un tratamiento a gran escala de categorías especiales de datos personales, el responsable que lo lleve a cabo deberán designar un delegado obligatoriamente
- D
- GDPR: 1
- GDPR_art: 37

DPO_CONTACT
- La ley determina que el responsable o el encargado del tratamiento publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control.
- D
- GDPR: 1
- GDPR_art: 37

DPO_TASKS
- La ley determina cuáles son las funciones mínimas que deberá tener el Delegado.
- D
- GDPR: 1
- GDPR_art: 39

Códigos de conducta (CODES)

CODE_EXIST
- La ley contempla la existencia de códigos de conducta elaborados por organismos representativos de categorías de responsables, en los cuales se especifique la aplicación de la ley. Comprenden acciones concretas donde se materializa la protección codificada en la ley.
- D
- GDPR: 1
- GDPR_art: 40

CODE_S
- La ley contempla que la autoridad de control podrá acreditar organismos para supervisar el cumplimiento de un código de conducta
- D
- GDPR: 1
- GDPR_art: 41

Certificación ()

CERTIFICATION
- La ley establece la posibilidad de creación de sellos, marcas o registro de organizaciones y/o empresas que cumplen con estándares de protección de datos.

- D
- GDPR: 1
- GDPR_art: 42

CERTIFICATION_BODY
- La ley contempla la existencia de organismos a los cuales la autoridad de control dio la potestad de certificar que una organización o empresa cumple con estándares de protección de datos
- D
- GDPR: 1
- GDPR_art: 42

Transferencia de datos personales a terceros países u organizaciones internacionales

TRANSF_EXIST
- La ley contempla y regula en alguna medida la transferencia de datos personales a terceros países u organizaciones internacionales
- D

TRANSF_ADEQUACY
- La ley contempla que se deberá, antes de transferir datos personales a otro país u organización, decidir si el mismo puede cumplir estándares de protección adecuados.

TRANSF_ADEQUACY_AUTH
- La ley determina que será la autoridad de control quien deberá tomar una decisión sobre la adecuación de los estándares de protección de un tercer país u organización internacional

ADEQUACY_ROL
- La ley determina que, al evaluar si un país u organización cumple con estándares de protección adecuados, tendrá en cuenta el “Rule Of Law”.

ADEQUACY_HR
- La ley determina que, al evaluar si un país u organización cumple con estándares de protección adecuados, tendrá en cuenta estándares de Derechos Humanos
- D
- GDPR: 1

- GDPR_art: 45

ADEQUACY_DPL
- La ley determina que, al evaluar si un país u organización cumple con estándares de protección adecuados, tendrá en cuenta las normas de protección de datos del país u organización de destino.
- D
- GDPR: 1
- GDPR_art: 45

ADEQUACY_AUTH
- La ley determina que, al evaluar si un país u organización cumple con estándares de protección adecuados, tendrá en cuenta la existencia y funcionamiento efectivo de uno o varias autoridades de control independientes
- D
- GDPR: 1
- GDPR_art: 45

ADEQUACY_TREATIES
- La ley determina que, al evaluar si un país u organización cumple con estándares de protección adecuados, tendrá en cuenta los compromisos internacionales asumidos por el tercer país u organización internacional
- D
- GDPR: 1
- GDPR_art: 45

INT_COOP
- La ley determina que las sentencias de órganos jurisdiccionales o las decisiones de autoridades administrativas de un tercer país que exijan la transferencia de datos personales a un responsable o encargado con base en el país de orígen solo será reconocida o ejecutable si se basa en un acuerdo internacional
- D
- GDPR: 1
- GDPR_art: 48

Normas corporativas

BIND_C_RULES

- La ley contempla la existencia de normas corporativas vinculantes, comprendidas como reglas internas de las empresas y organismos que dictan cómo se realizan los tratamientos.re
- D
- GDPR: 1
- GDPR_art: 47

Autoridades de control independientes

AUTH_EXIST

- La ley determina o crea autoridades públicas, a las cuales asigna la responsabilidad por sobre la aplicación de la ley de protección de datos.
- D
- GDPR: 1
- GDPR_art: 51

AUTH_MULTI

- La ley contempla la creación de más de una autoridad de control
- D
- GDPR: 1
- GDPR_art: 51

AUTH_HIERARCHY

- La ley dispone que, cuando haya varias autoridades de control en un mismo Estado, este Estado designará la autoridad de control que representará a dichas autoridades en el Comité
- D
- GDPR: 1
- GDPR_art: 51

AUTH_IND

- La ley determina que la autoridad de control será independiente en su accionar
- D
- GDPR: 1
- GDPR_art: 52

AUTH_HIRE
- La ley determina que la autoridad de control seleccionará y dispondrá de forma exclusiva de su personal
- D
- GDPR: 1
- GDPR_art: 52

AUTH_BUDGET
- La ley determina que la autoridad de control tendrá su propio presupuesto anual, contribuyendo a su independencia económica
- D
- GDPR: 1
- GDPR_art: 52

AUTH_DES
- La ley define el método de designación de, al menos, la persona a cargo de la autoridad de control principal
- D
- GDPR: 1
- GDPR_art: 53

AUTH_MANDATE
- La ley determina la duración del mandato de la persona a cargo de la autoridad de control (el cargo tiene mandato fijo).
- D
- GDPR: 1
- GDPR_art: 54

AUTH_RENEW
- La ley determina que la persona a cargo de la autoridad de control puede ser reelecta.
- D
- GDPR: 1
- GDPR_art: 54

AUTH_REGISTER
- La ley contempla la creación de registros declarativos de bases de datos y archivos.
- D

GDPR: 0

AUTH_COMP
- La ley determina la competencia de la autoridad de control.
- D
- GDPR: 1
- GDPR_art: 56

AUTH_GOV
- La ley determina que cualquier tratamiento llevado a cabo por autoridades públicas será competentecia de la autoridad de control.
- D
- GDPR: 1
- GDPR_art: 55

AUTH_JUDICIARY
- La ley determina que las autoridades de control no serán competentes para controlar las operaciones de tratamiento efectuadas por los tribunales en el ejercicio de su función judicial.
- D
- GDPR: 1
- GDPR_art: 55

AUTH_REC
- La ley determina que la autoridad de control será competente para tratar una reclamación que le sea presentada o una posible infracción de la ley.
- D
- GDPR: 1
- GDPR_art: 56

AUTH_IP_ORDER
- La ley determina que la autoridad tendrá la potestad de ordenar al responsable y al encargado del tratamiento que faciliten cualquier información que requiera para el desempeño de sus funciones
- D
- GDPR: 1
- GDPR_art: 58

AUTH_IP_AUDIT

- La ley determina que la autoridad tendrá la potestad de realizar investigaciones en forma de auditorías
- D
- GDPR: 1
- GDPR_art: 58

AUTH_IP_CERT

- La ley determina que la autoridad tendrá la potestad de llevar adelante la revisión de las certificaciones.
- D
- GDPR: 1
- GDPR_art: 58

AUTH_IP_NOTIF

- La ley determina que la autoridad tendrá la potestad de notificar al responsable o al encargado del tratamiento las presuntas infracciones.
- D
- GDPR: 1
- GDPR_art: 58

AUTH_IP_ACCESSD

- La ley determina que la autoridad tendrá la potestad de obtener acceso a todos los datos personales y a toda la información necesaria para el ejercicio de sus funciones;
- D
- GDPR: 1
- GDPR_art: 58

AUTH_IP_ACCESSE

- La ley determina que la autoridad tendrá la potestad de obtener el acceso a todos los locales del responsable y del encargado del tratamiento
- D
- GDPR: 1
- GDPR_art: 58

AUTH_CP_WARN

- La ley determina que la autoridad tendrá la potestad de sancionar a todo responsable o encargado del tratamiento con una **advertencia** cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto

- D
- GDPR: 1
- GDPR_art: 58.2

AUTH_CP_REPR
- La ley determina que la autoridad tendrá la potestad de sancionar a todo responsable o encargado del tratamiento con **apercibimiento** cuando las operaciones de tratamiento hayan infringido lo dispuesto
- D
- GDPR: 1
- GDPR_art: 58.2

AUTH_CP_REQ
- La ley determina que la autoridad tendrá la potestad de **ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos del interesado**
- D
- GDPR: 1
- GDPR_art: 58.2

AUTH_CP_COMPLY
- La ley determina que la autoridad tendrá la potestad de ordenar se ajusten a las disposiciones de la ley
- D
- GDPR: 1
- GDPR_art: 58.2

AUTH_CP_COMM
- La ley determina que la autoridad tendrá la potestad de ordenar al responsable del tratamiento que comunique al interesado las violaciones de la seguridad de los datos personales;
- D
- GDPR: 1
- GDPR_art: 58.2

AUTH_CP_BAN
- La ley determina que la autoridad tendrá la potestad de imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición;
- D
- GDPR: 1

- GDPR_art: 58.2

AUTH_CP_ERASE
- La ley determina que la autoridad tendrá la potestad de ordenar la rectificación o supresión de datos personales o la limitación de tratamiento y la notificación de dichas medidas a los destinatarios
- D
- GDPR: 1
- GDPR_art: 58.2

AUTH_CP_WDW
- La ley determina que la autoridad tendrá la potestad de retirar una certificación
- D
- GDPR: 1
- GDPR_art: 58.2

AUTH_CP_AFINE
- La ley determina que la autoridad tendrá la potestad de imponer una multa administrativa
- D
- GDPR: 1
- GDPR_art: 58.2

AUTH_CP_EXPORT
- La ley determina que la autoridad tendrá la potestad de ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país
- D
- GDPR: 1
- GDPR_art: 58.2

AUTH_AAP_ADV
- La ley determina que la autoridad tendrá la potestad de asesorar al responsable del tratamiento conforme al procedimiento de consulta previa
- D
- GDPR: 1
- GDPR_art: 58.3

AUTH_AAP_LEG

- La ley determina que la autoridad tendrá la potestad de emitir, por iniciativa propia o previa solicitud, opiniones destinados al Parlamento nacional, al Gobierno del Estado miembro
- D
- GDPR: 1
- GDPR_art: 58.3

AUTH_AAP_ISSUE1

- La ley determina que la autoridad tendrá la potestad de emitir un dictamen y aprobar proyectos de códigos de conducta
- D
- GDPR: 1
- GDPR_art: 58.3

AUTH_AAP_ISSUE2

- La ley determina que la autoridad tendrá la potestad de acreditar los organismos de certificación
- D
- GDPR: 1
- GDPR_art: 58.3

AUTH_AAP_ISSUE3

- La ley determina que la autoridad tendrá la potestad de expedir certificaciones
- D
- GDPR: 1
- GDPR_art: 58.3

AUTH_JUDICIAL

- La ley determina que la autoridad tendrá la potestad de iniciar o ejercitar de otro modo acciones judiciales, con el fin de hacer cumplir lo dispuesto en el mismo
- D
- GDPR: 1
- GDPR_art: 58.5

Conciliación

FREESPEECH_EXIST

- La ley contempla, incluye o realiza observaciones respecto del derecho a la libre expresión.

- D
- GDPR: 1
- GDPR_art: 85

FREESPEECH_EXCEPT
- La ley incluye exenciones o excepciones a lo dispuesto por la misma si son necesarias para conciliar el derecho a la protección de los datos personales con la libertad de expresión e información
- D
- GDPR: 1
- GDPR_art: 85

ID_EXIST
- condiciones específicas para el tratamiento de un número nacional de identificación o cualquier otro medio de identificación de carácter general
- D
- GDPR: 1
- GDPR_art: 87

WORKPLACE_EXIST
- normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral
- D
- GDPR: 1
- GDPR_art: 88

REPEAL
- Anula o deroga algún tipo de legislación previa
- D
- GDPR: 1
- GDPR_art: 94

TREATIES
- Contempla la conciliación con acuerdos internacionales que impiquen la transferencia de datos personales a terceros países u organizaciones internacionales que hubieren sido celebrados.
- D
- GDPR: 1
- GDPR_art: 96

Otras

CRIMINAL_CONS

- La ley determina consecuencias penales para quienes la incumplen?
    - D
    - GDPR: 0

ECONOMIC_CONS

- La ley determina consecuencias económicas para quienes la incumplen?
- D
- GDPR: 1

FINES_AUTH

- cada autoridad de control garantizará la imposición de las multas administrativas
- D
- GDPR: 1
- GDPR_art: 83

AUTH_CP_AFINE

- imponer una multa administrativa
- D
- GDPR: 1
- GDPR_art: 58.2

FED_UNI

- La variable estudia si el país en el que se sancionó la ley analizada es un régimen federal o unitario.
- En esta variable discreta, el valor "1" representa "Federal", mientras que el "0" representa "Unitario".
- D

COMMONWEALTH

- La variable estudia si el país en el que se sancionó la ley analizada pertenece a la Commonwealth.
- En esta variable discreta, el valor "1" representa "Si", mientras que el "0" representa "No".
- D

Variables tomadas de bases de datos:

Variables tomadas de la base de datos V-Dem

LIBDEM

- Base de datos original: V-Dem [Country-Year/Country-Date] Dataset v13
- Título en base original: Liberal democracy index (D) (v2x_libdem)
- Project Manager(s): Jan Teorell
- Question: To what extent is the ideal of liberal democracy achieved?
- Clarification: The liberal principle of democracy emphasizes the importance of protecting individual and minority rights against the tyranny of the state and the tyranny of the majority. The liberal model takes a "negative" view of political power insofar as it judges the quality of democracy by the limits placed on government. This is achieved by constitutionally protected civil liberties, strong rule of law, an independent judiciary, and effective checks and balances that, together, limit the exercise of executive power. To make this a measure of liberal democracy, the index also takes the level of electoral democracy into account.
- Scale: Interval, from low to high (0-1).
- Source(s): v2x_liberal v2x_polyarchy
- Data release: 1-13. Release 1, 2, and 3 used a different, preliminary aggregation formula.
- `Aggregation: The index is aggregated using this formula: v2x_libdem =.25 * v2x_polyarchyl.585 + .25 * v2x_liberal + .5 * v2x_polyarchyl.585 * v2x_liberal`
- Citation: Coppedge et al. (2015, V-Dem Working Paper Series 2015:6); V-Dem Codebook

Variables tomadas de la base de datos Quality of Government

- POP2019
- Base de datos original: Quality of Government Cross Section January 2023
- Título en base original: Population, total (wdi_pop)
- Dataset del cual fue extraído por QoG: World Development Indicators
- Description: Total population is based on the de facto definition of population, which counts all residents regardless of legal status or citizenship. The values shown are midyear estimates.

ANEXO II: Tablas con composición de índices

CÓDIGO DEL ÍNDICE	VARIABLE	DESCRIPCIÓN DE LA VARIABLE
INDEX_CONSENT	CONSENT_EASE	Determina que el contexto en el que el interesado brinda consentimiento para el tratamiento de sus datos personales debe presentar lenguaje claro y ser de fácil acceso
	CONSENT_WD	La ley determina que será **tan fácil retirar el consentimiento como darlo**
	CONSENT_AGE	El consentimiento solo puede ser brindado por **mayores de una determinada edad,** y el consentimiento de menores solo puede ser brindado por los titulares de la patria potestad o tutela sobre el niño

ÍNDICE	VARIABLE	DESCRIPCIÓN DE LA VARIABLE
INDEX_INSTRUMENTS	DS_R_ADMIN	El interesado puede comenzar una acción administrativa ante el incumplimiento de la ley?
	DS_R_JUDICIAL	El interesado puede comenzar una acción judicial ante el incumplimiento de la ley?
	DS_R_REMEDYAUTH	toda persona física o jurídica tendrá derecho a la tutela judicial contra una decisión jurídicamente vinculante de una autoridad de control que le concierna
	DS_R_REMEDYCONTROLLER	todo interesado tendrá derecho a la tutela judicial efectiva cuando considere que sus derechos en virtud de la ley han sido vulnerados como consecuencia de un tratamiento de sus datos personales.
	DS_R_REMEDYCONTROLLER2	Las acciones contra un responsable o encargado se ejercitan ante los tribunales del estado en donde el responsable tiene establecimiento
	DS_R_REPRESENTANT	El interesado tendrá derecho a dar mandato a una entidad, organización o asociación para que presente en su nombre una reclamación, y ejerza en su nombre los derechos y el derecho a ser indemnizado
	DS_R_COMPENSATION	Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos.

ÍNDICE	VARIABLE	DESCRIPCIÓN DE LA VARIABLE
	DS_INF_RECL	La ley determina que, en caso de ser obtenidos por vía del interesado, el responsable informará al interesado en el momento de la obtención de los datos la existencia del **derecho a presentar una reclamación ante**
	DS_R_PROCESS	La ley determina que el interesado tiene derecho a saber si sus datos personales están siendo tratados.
	DS_R_OBJ	La ley dispone que el interesado tiene derecho a conocer cuáles son los fines que persigue el responsable o encargado a la hora de tratar sus datos
	DS_R_DES	La ley determina que el interesado tiene **derecho a conocer quienes son los destinatarios de sus datos personales,** sean estos terceros u
	DS_R_ORIGIN	La ley **determina que el interesado tiene derecho a conocer cualquier información disponible sobre el origen de los datos personales cuando estos no se hayan**
	DS_R_AUTO	La ley determina que el interesado tiene **derecho a saber de la existencia de decisiones automatizadas, incluída la elaboración de**
	DS_R_COPY	La ley determina que el interesado tiene derecho a recibir una copia de los datos personales objeto de tratamiento por parte del responsable de tratamiento.
	DS_R_OPO1	La ley determina que el interesado tiene derecho a oponerse al tratamiento de sus datos personales si el mismo tiene como objeto la mercadotecnia directa, incluida la elaboración de perfiles
	DS_R_OPO2	La ley determina que el interesado tiene derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.
	DS_R_SUPR_PUBLIC	La ley determina que, **cuando el responsable haya hecho públicos sus datos personales, el interesado tiene derecho a que el responsable aplique medidas razonables para hacer saber a otros responsables que estén tratando esos datos de la solicitud del**

ÍNDICE	VARIABLE	DESCRIPCIÓN DE LA VARIABLE
INDEX_RIGHTS	TRANSPARENT_INFO	El responsable debe **brindar información al interesado de forma transparente, concisa, inteligible y de fácil acceso, lenguaje claro y**
	DS_INF_TRTMT	El interesado debe ser informado sobre el tratamiento de sus datos personales?
	DS_INF_TRANSF	La ley determina que, en caso de ser obtenidos por vía del interesado, el responsable informará al interesado en el momento de la obtención de los datos, en su caso, la **intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o**
	DS_INF_TERM	La ley determina que, en caso de ser obtenidos por vía del interesado, el responsable informará al interesado en el momento de la obtención de los datos **el plazo durante el cual se conservarán los datos personales** o, cuando no sea posible, los criterios
	DS_INF_ALT	La ley determina que, cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional
	DS_INF_RIGHTS	El interesado debe ser informado de sus derechos a la hora de dar consentimiento para el tratamiento?
	DS_INF_RECTIF	La ley determina que, en caso de ser obtenidos por vía del interesado, el responsable informará al interesado en el momento de la obtención de los datos la existencia del **derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento. o a oponerse al tratamiento. así**
	DS_INF_CONSWD	La ley determina que, en caso de ser obtenidos por vía del interesado, el responsable informará al interesado en el momento de la obtención de los datos la existencia del **derecho a retirar el consentimiento en cualquier momento**, sin que ello afecte a la licitud del tratamiento basado en el

ÍNDICE	VARIABLE	DESCRIPCIÓN DE LA VARIABLE
INDEX_AUTH	AUTH_IND	La ley determina que la autoridad de control será independiente en su accionar
	AUTH_BUDGET	La ley determina que la autoridad de control tendrá su propio presupuesto anual, contribuyendo a su independencia económica
	AUTH_DES	La ley define el método de designación de, al menos, la persona a cargo de la autoridad de control principal
	AUTH_MANDATE	La ley determina la duración del mandato de la persona a cargo de la autoridad de control (el cargo tiene
	AUTH_RENEW	La ley determina que la persona a cargo de la autoridad de control puede ser reelecta.
	AUTH_REGISTER	La ley contempla la creación de registros declarativos de bases de datos y archivos.
	AUTH_COMP	La ley determina la competencia de la autoridad de
	AUTH_GOV	La ley determina que cualquier tratamiento llevado a cabo por autoridades públicas será competentecia de la autoridad de control.
	AUTH_REC	La ley determina que la autoridad de control será competente para tratar una reclamación que le sea presentada o una posible infracción de la ley.
	AUTH_IP_ORDER	La ley determina que la autoridad tendrá la potestad de ordenar al responsable y al encargado del tratamiento que faciliten cualquier información que requiera para el desempeño de sus funciones
	AUTH_IP_AUDIT	La ley determina que la autoridad tendrá la potestad de realizar investigaciones en forma de auditorías
	AUTH_IP_NOTIF	La ley determina que la autoridad tendrá la potestad de notificar al responsable o al encargado del tratamiento las presuntas infracciones.
	AUTH_IP_ACCESSD	La ley determina que la autoridad tendrá la potestad de obtener acceso a todos los datos personales y a toda la información necesaria para el ejercicio de sus
	AUTH_IP_ACCESSE	La ley determina que la autoridad tendrá la potestad de obtener el acceso a todos los locales del responsable y del encargado del tratamiento
	AUTH_CP_WARN	La ley determina que la autoridad tendrá la potestad de sancionar a todo responsable o encargado del tratamiento con una **advertencia** cuando las operaciones de tratamiento previstas puedan infringir lo
	AUTH_CP_REPR	La ley determina que la autoridad tendrá la potestad de sancionar a todo responsable o encargado del tratamiento con **apercibimiento** cuando las operaciones de tratamiento hayan infringido lo
	AUTH_CP_COMPLY	La ley determina que la autoridad tendrá la potestad de ordenar se ajusten a las disposiciones de la ley
	AUTH_CP_BAN	La ley determina que la autoridad tendrá la potestad de imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición;
	AUTH_CP_ERASE	La ley determina que la autoridad tendrá la potestad de ordenar la rectificación o supresión de datos personales o la limitación de tratamiento y la notificación de dichas medidas a los destinatarios
	AUTH_CP_AFINE	La ley determina que la autoridad tendrá la potestad de imponer una multa administrativa
	AUTH_JUDICIAL	La ley determina que la autoridad tendrá la potestad de iniciar o ejercitar de otro modo acciones judiciales, con el fin de hacer cumplir lo dispuesto en el mismo
	AUTH_AAP_LEG	La ley determina que la autoridad tendrá la potestad de emitir, por iniciativa propia o previa solicitud, opiniones destinados al Parlamento nacional, al Gobierno del
	AUTH_AAP_ISSUE1	La ley determina que la autoridad tendrá la potestad de emitir un dictamen y aprobar proyectos de códigos de

ÍNDICE	VARIABLE	DESCRIPCIÓN DE LA VARIABLE
INDEX_TRANSF	TRANSF_EXIST	La ley contempla y regula en alguna medida la transferencia de datos personales a terceros países u organizaciones internacionales
	TRANSF_ADEQUACY	La ley contempla que se deberá, antes de transferir datos personales a otro país u organización, decidir si el mismo puede cumplir estándares de protección adecuados.
	ADEQUACY_DPL	La ley determina que, al evaluar si un país u organización cumple con estándares de protección adecuados, tendrá en cuenta las normas de protección de datos del país u organización de destino.
	ADEQUACY_AUTH	La ley determina que, al evaluar si un país u organización cumple con estándares de protección adecuados, tendrá en cuenta la existencia y funcionamiento efectivo de uno o varias autoridades de control independientes
	ADEQUACY_TREATIES	La ley determina que, al evaluar si un país u organización cumple con estándares de protección adecuados, tendrá en cuenta los compromisos internacionales asumidos por el tercer país u organización internacional
	INT_COOP	La ley determina que las sentencias de órganos jurisdiccionales o las decisiones de autoridades administrativas de un tercer país que exijan la transferencia de datos personales a un responsable o encargado con base en el país de origen solo será reconocida o ejecutable si se basa en un acuerdo internacional

ÍNDICE	VARIABLE	DESCRIPCIÓN DE LA VARIABLE
INDEX_DPO	DPO_EXIST	La ley contempla la figura de un delegado de tratamiento, entendido como una persona de la nómina del responsable o quien opera bajo contrato de servicio, a quien se delegan las actividades de protección de
	DPO_IND	La ley determina que el delegado no puede recibir instrucciones sobre su labor, ser destituido ni
	DPO_DESIGNATION_COMP	La ley determina que, para al menos un tipo de tratamiento, los responsables que lo lleven a cabo deberán designar un delegado obligatoriamente
	DPO_DESIGNATION_SCALE	La ley determina que, cuando el tratamiento requiera observación habitual y sistemática de interesados a gran escala, los responsables que lo lleven a cabo deberán designar un delegado obligatoriamente
	DPO_DESIGNATION_SPCAT	La ley determina que, cuando el responsable lleve a cabo un tratamiento a gran escala de categorías especiales de datos personales, el responsable que lo lleve a cabo deberán designar un delegado
	DPO_CONTACT	La ley determina que el responsable o el encargado del tratamiento publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control.
	DPO_TASKS	La ley determina cuáles son las funciones mínimas que deberá tener el Delegado.

ÍNDICE	VARIABLE	DESCRIPCIÓN DE LA VARIABLE
INDEX_DCDP	REPRESENTATIVE	La ley establece que, cuando el responsable del tratamiento no reside en el pais, deberá establecer un representante en el pais. El responsable atiende junto al responsable o encargado a las consultas de la autoridad de control y de los
	PROCESSOR	La ley determina que el responsable del tratamiento podrá recurrir a un encargado para el procesamiento de los datos siguiendo instrucciones documentadas, incluyendo transferencias.
	PROCESSOR_CONTRACT	La ley determina que el responsable del tratamiento podrá recurrir a un encargado con contrato de por medio
	PROCESSOR_OTHER	La ley determina que el encargado no recurre a otro encargado sin permiso del responsable
	PROCESSOR_ASSURANCES	La ley dicta que el encargado deberá tomar medidas para garantizar seguridad y confidencialidad en el tratamiento
	TRTMT_REGISTER	La ley dicta que responsables y encargados deberán registrar las actividades de tratamiento efectuadas bajo su responsabilidad
	BREACH_AUT	La ley determina que, ante una violación a la seguridad de los datos personales, el responsable de tratamiento deberá notificarla a la autoridad de control competente.
	BREACH_DS	Ante una violación de la seguridad de los datos personales que entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable la comunicará al interesado sin dilación.
	I_ASSESMENT	La ley determina que, cuando es probable que un tratamiento entrañe riesgos a derechos o libertades de personas físicas, se hace evaluación de impacto de las operaciones de tratamiento. Esto comprende procesos de prevención y mitigación de riesgos.

ANEXO III: Base de datos sobre leyes de protección de datos en América Latina y el Caribe

Por cuestiones de espacio y formato del archivo, no es posible insertar la base de datos construida en el presente documento. Sin embargo, se dejará aquí[63] citado un link con acceso público a la base. Al igual que con el resto de la presente tesis de grado, deberá citarse cualquier elemento extraído de la misma.

63 https://docs.google.com/spreadsheets/d/1CreAZNSYkRLNHAgqkmn6NFKX5QIoJys_/edit?usp=sharing&ouid=115941295637011783236&rtpof=true&sd=true