Guía para la implementación de una política pública de protección de datos

EL SALVADOR

IPANDETEC
CENTROAMÉRICA

Edición: Aquilino Rodríguez
Diagramación: Juan Pablo Hoyos C.
Coordinación: Abdías Zambrano
Investigación y revisión realizada con la cooperación del International Human Rights Advocates at the University of Pennsylvania Law School

IPANDETEC
CENTROAMÉRICA

IPANDETEC Centroamérica es una organización sin fines de lucro, basada en la Ciudad de Panamá, que promueve el uso y regulación de las TIC y la defensa de los Derechos Humanos en el entorno digital a través de la incidencia, investigación, monitoreo y seguimiento legislativo de Políticas Públicas de Internet en Centroamérica.

Este policy paper se realizó gracias al apoyo del Fondo Indela.

I. INTRODUCCIÓN

Al igual que en otros países de América Central, al redactar este 'policy paper' El Salvador todavía carece de una ley integral de protección de datos. En los últimos dos años se han realizado avances significativos hacia la legislación, pero ha sido a costa de la participación de múltiples partes interesadas y de una cuidadosa consideración. En particular, el tema de la protección de datos ha presentado desafíos particulares en una sociedad cada vez más digitalizada, definida por las transacciones e intercambios diarios de información. La privacidad de los datos plantea cuestiones relativas a la seguridad, la calidad de los datos, la transparencia y el acceso a la información, entre otras importantes consideraciones normativas.

En este documento, ofrecemos una visión general del régimen actual de protección de datos de El Salvador, una revisión del proyecto de ley de protección de datos que se discutió en la Asamblea, y recomendaciones para que las partes interesadas salvadoreñas ayuden a garantizar que los esfuerzos de protección de datos, ahora o en el futuro, respeten los derechos humanos fundamentales.

II. LA REGULACIÓN NACIONAL

Los derechos a la dignidad están consagrados en el artículo 2 de la Constitución de El Salvador.[1] Los tribunales de El Salvador han utilizado el artículo 2 para respaldar los derechos de datos a través de un derecho de "autodeterminación informativa" inferido en el país.

Jurisprudencia e interpretación constitucional

La Sala de lo Constitucional de la Corte Suprema de Justicia de El Salvador estableció el derecho a la "autodeterminación informativa" en un caso histórico de 2004.[2] Boris Rubén Solórzano representó a la Asociación Salvadoreña para la Protección de Datos e Internet ('INDATA') en una demanda contra Equifax Centroamérica, conocida como DICOM.[3] La empresa había estado recopilando y comercializando información crediticia personal de ciudadanos salvadoreños sin su conocimiento ni consentimiento.

1. Constitución de El Salvador, art. 2, 1983, modificada en 2003.
2. Centro de Información sobre Privacidad Electrónica, 2006, El Salvador, Informe sobre Privacidad y Derechos Humanos, http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-El.html#fn2125.
3. Zaragoza Canales, O. Ramos Romero, I. Carias Soriano, J. Septiembre 2015. La regulación del Habeas Data como mecanismo de protección de los ciudadanos y su derecho a la autodeterminación informativa. http://ri.ues.edu.sv/id/eprint/11551/1/50108248.pdf

En su lucha por el derecho a la intimidad en una época de tecnología prolífica, el tribunal sentó un importante precedente en materia de privacidad de varias maneras.[4] En primer lugar, reconoció el derecho de todos los ciudadanos a acceder a su información personal, especialmente la que se almacena en bases de datos informáticas. En segundo lugar, interpretó este derecho en el sentido de que todo sujeto a datos que debe tener la capacidad y el derecho de controlar razonablemente la distribución y transmisión de cualquier información que le concierna. En tercer lugar, pidió la creación de un procedimiento que proporcione medios efectivos de reparación a aquellos cuyos derechos hayan sido violados. En cuarto lugar, establece el derecho al olvido, sosteniendo que toda información crediticia de un individuo que se almacene en una base de datos que debe ser eliminada un determinado tiempo después de su creación. Por último, señaló que cualquier uso o tratamiento de la información personal por parte de terceros debe estar justificado.

Autoridad reguladora

En la actualidad, El Salvador no cuenta con una autoridad designada para la protección de datos personales, durante la discusión del proyecto de ley de datos personales se discutió también la creación de una Agencia Nacional Digital. El gobierno de El Salvador creó el Instituto de Acceso a la Información Pública (un organismo público conocido como IAIP) a través de la Ley de Acceso a la Información Pública. El Instituto tiene como misión "Garantizar el ejercicio del derecho de acceso a la información pública y la protección de datos personales con independencia, calidad e innovación, y en coordinación interinstitucional". En marzo de 2020, el IAIP publicó directrices para la protección de datos personales durante la pandemia.[5] Además, la Dirección de Protección al Consumidor de El Salvador ha asumido funciones especiales de protección de datos.

Legislación relacionada/adyacente

En El Salvador existen varias leyes que afectan a la protección de datos personales y la jurisprudencia correspondiente.

La Ley de Protección del Consumidor

La Ley de Protección de los Consumidores exige a las entidades comerciales que consideren la información personal como confidencial y tomen medidas para salvaguardar los datos personales privados.[6] Esta ley fue modificada en 2018 para incluir el comercio electrónico. Los principales artículos que regulan el comercio electrónico son los artículos 21, 21-A y 22. La ley también se actualizó en 2020, en gran medida en respuesta a la pandemia de Coronavirus.

4. Sentencia del Tribunal Supremo 142-2012, Las Asociación Salvadoreña para la Protección de Datos e Internet v. DICOM, 2004, https://www.jurisprudencia.gob.sv/DocumentosBoveda/D/1/2010-2019/2014/10/AA0E4.PDF.

5. Instituto de Acceso a la Información Pública. Lineamientos generales de protección de datos personales para las instituciones que conforman el sector público. https://www.transparencia.gob.sv/institutions/iaip/documents/otros-documentos-normativos

6. Ley de Protección del Consumidor. Modificado 2021. https://www.defensoria.gob.sv/wp-content/uploads/2015/04/LEY-DE-PROTECCIO%CC%81N-AL-CONSUMIDOR-CON-REFORMAS-2020-WEB-1.pdf

Ley de regulación de los servicios de información sobre el historial de crédito personal (2011)

Esta ley se desarrolló en respuesta a la decisión del Tribunal Supremo en el caso INDATA contra DICOM. Esta sentencia estableció varios principios fundamentales:[7]

- El acceso de la persona autorizada: Una persona tiene derecho a saber si una empresa tiene y trata sus datos de crédito. También tiene derecho a que se actualicen esos datos cuando sean incorrectos, injustificados, inexactos o defectuosos.

- La calidad de los datos: La información tratada por una entidad de crédito comercial debe ser correcta y estar actualizada.

- Confidencialidad: Cualquier persona con acceso a la información crediticia no puede revelarla o darla a terceros, excepto a las autoridades gubernamentales o a las entidades que participan en las operaciones de una agencia de información.

- Seguridad: Los comerciantes de información crediticia deben adoptar medidas o controles técnicos para evitar la modificación no autorizada o la pérdida de información crediticia.

El Código Penal (1997) (artículos 184-186)

El código penal de 1997 tipifica como delito la invasión de la intimidad de otras personas mediante la toma de posesión de sus datos confidenciales y personales. La ley incluye, los datos personales disponibles en bases de datos públicas o privadas. La ley también penaliza la posesión ilegal de comunicaciones escritas u otros documentos confidenciales y personales. El código penal establece penas leves por revelar datos personales a terceros, y establece penas graves si la persona que revela los datos es un controlador de datos, un procesador de datos u otra persona de confianza con un trabajo especializado en la seguridad de la información.

El código también protege las telecomunicaciones. Cualquiera que intercepte, impida o interrumpa las comunicaciones telegráficas o telefónicas está sujeto a sanciones penales. Además, quien utilice herramientas o dispositivos para espiar las comunicaciones telefónicas, transmitir sonido o recordar las comunicaciones telefónicas con el fin de entrometerse en la intimidad de los demás está sujeto a graves sanciones penales, como de seis meses a un año de prisión.

7. Guía de datos. Panorama de la protección de datos en El Salvador. https://www.dataguidance.com/notes/el-salvador-data-protection-overview

Ley de Acceso a la Información Pública (2011)

Esta ley otorga a los individuos salvadoreños el derecho a obtener información pública del gobierno y otras autoridades públicas. La ley también incluye disposiciones sobre la protección de los datos personales en el contexto de las operaciones gubernamentales.

Ley especial contra los delitos informáticos y conexos (2016)

Esta ley regula el uso no autorizado de datos personales resultantes del acceso ilegal a bases de datos informáticas. Además, la ley penaliza otras acciones indebidas relacionadas con las tecnologías de la información y la comunicación.

Ley de Protección Integral de la Niñez y la Adolescencia (2009)

Esta ley fue uno de los primeros esfuerzos de El Salvador para controlar a los niños que utilizan Internet. La ley prohíbe el uso, la divulgación, la publicación o la exposición de datos, imágenes u otra información de un niño o adolescente sin el permiso o el conocimiento de los padres o tutores, y de manera que perjudique y dañe la reputación o el honor del niño. Al igual que el código penal que tipifica como delito las acciones destinadas a invadir la intimidad de otras personas, esta ley tipifica como delito las acciones con datos personales de los niños que interfieren en la intimidad del niño o de la familia de forma ilícita o arbitraria.

III. BREVE REVISIÓN DE LA NORMATIVA INTERNACIONAL

Organización de Estados Americanos

La Convención Americana sobre Derechos Humanos de 1969, más conocida como Pacto de San José de Costa Rica, establece en su artículo 11 que toda persona tiene derecho a que se respete su honra y se reconozca su dignidad, y menciona también que toda persona tiene derecho a la protección de la ley contra esas injerencias o ataques. Este derecho es fundamental para la protección de datos.[8]

Desde 1996, la Asamblea General (AG) de la OEA viene aprobando resoluciones en materia de protección de datos personales.[9]

8. Convención Americana de Derechos Humanos. (1969). https://www.oas.org/dil/esp/tratados_b-32_convencion_americana_sobre_derechos_humanos.html
9. Organización de Estados Americanos. (2009, 1 de agosto). Protección de datos personales. http://www.oas.org/es/sla/ddi/proteccion_datos_personales.asp

El tema también ha estado en la agenda del Comité Jurídico Interamericano, que en el año 2000 presentó un documento sobre "El derecho a la información: Acceso y protección de la información y datos personales en formato electrónico".[10] Desde ese año, el Comité Jurídico Interamericano continuó trabajando en esta área, adoptando una serie de documentos. Particularmente, en 2012, el Comité Jurídico Interamericano aprobó una "Propuesta de Declaración de Principios sobre Privacidad y Protección de Datos Personales en las Américas", que contiene 12 principios sobre el tema, y en 2015, la "Guía Legislativa sobre Privacidad y Protección de Datos Personales en las Américas."[11]

Recientemente, la Asamblea General (AG) solicitó al Comité Jurídico Interamericano que iniciara la actualización de los Principios sobre la Protección de Datos Personales, teniendo en cuenta su evolución, tarea que el Comité Jurídico Interamericano está llevando a cabo con el apoyo del Departamento de Derecho Internacional en su calidad de Secretaría Técnica.[12]

La Corte Interamericana de Derechos Humanos (Corte IDH), por turnos, fue establecida para conocer casos en el marco de la Convención Americana de Derechos Humanos y para interpretar los derechos adjudicados bajo su poder.[13] Sin embargo, debido a que la Corte se estableció por primera vez en un contexto histórico de "inestabilidad política, violencia y agitación económica", gran parte de la jurisprudencia de la Corte se ha desarrollado en torno a casos anteriores y no ha indagado sustancialmente en los derechos derivados e imaginados en sus artículos.[14] A pesar de las escasas indagaciones del Tribunal sobre los derechos a la intimidad en materia de información, es probable que este tipo de casos surjan con más frecuencia.[15]

El Tribunal ha derivado otros derechos a la intimidad del artículo 11, incluidos los derechos reproductivos,[16] tratando el derecho a la intimidad como una importante protección contra la interferencia y la intrusión del Estado en la elección y la identidad.[17]

Con respecto a la protección de datos, el sistema interamericano de derechos humanos ha optado cada vez más por la estrategia de tratar el derecho a la protección de datos como una dimensión distinta del derecho a la privacidad, lo que ha dado lugar a un mayor número de legislaciones nacionales que garantizan ambos derechos de acuerdo con las directrices y los principios interamericanos.[18]

10. Organización de Estados Americanos. (2012). Principios de la CJI. http://www.oas.org/es/sla/ddi/proteccion_datos_personales_Principios_CJI_2012.asp

11. Organización de Estados Americanos. (2015). Guía Legislativa del CJI. http://www.oas.org/es/sla/ddi/proteccion_datos_personales_Guia_Legislativa_CJI_2015.asp

12. Organización de Estados Americanos. (2009, 1 de agosto). Protección de datos personales. http://www.oas.org/es/sla/ddi/proteccion_datos_personales.asp

13. Wolfson, J. (2017). The expanding scope of human rights in a technological world-using the Inter-American Court of Human Rights to establish a minimum data protection standard across Latin America. University of Miami Inter-American Law Review, 18(3), 204-205 (https://www.jstor.org/stable/26788311).

14. Id.

15. Ver, por ejemplo, Escher et al. v. Brazil, IA Ct. H.R. (2009) (donde se encontró que las escuchas telefónicas injustificadas y el registro sin orden judicial equivalían a una violación del artículo 11).

16. Artavia Murillo y otros ("Fecundación in vitro") c. Costa Rica, Inter-Am. Ct. H. R. (ser. C) No. 257 (28 de noviembre de 2012).

17. Hevia, M. (2018). Gestación subrogada, privacidad y la Convención Americana de Derechos Humanos. Revista de Derecho y Biociencias, 5(2) (doi:10.1093/jlb/lsy013)

18. Véase en general Affonso Souza, C., de Oliveira, C. C., Perrone, C., & Carneiro, G. (2021). De la privacidad a la protección de datos: el camino a seguir por el Sistema Interamericano de Derechos Humanos. The International Journal of Human Rights, 25(1) (https://doi.org/10.1080/13642987.2020.1789108.)

Garantizar que todo el mundo pueda tener control sobre sus datos personales es posible, a través de los derechos que confieren los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), regulados por la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales.[19]

El derecho de acceso es el derecho de una persona a solicitar información al responsable de un fichero sobre el tratamiento de sus datos personales. El derecho de rectificación es el derecho del interesado a solicitar la modificación de los datos inexactos o incompletos. El derecho de oposición es el derecho de una persona a oponerse al tratamiento de sus datos personales o al cese de dicho tratamiento en determinados casos. Por último, el derecho de cancelación es aquel por el que el interesado puede solicitar la supresión de los datos que sean inadecuados o excesivos, sin perjuicio del deber de bloqueo.

Cabe mencionar en primer lugar que el ejercicio de estos derechos. es personal. En caso de que la solicitud no sea realizada por el interesado, su representante legal o un representante acreditado, el responsable del tratamiento podrá denegar la solicitud.

Privacidad y protección de datos personales en Europa

El artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales expresa el derecho de toda persona al respeto de su vida privada y familiar, así como de su domicilio y correspondencia.[20]

En mayo de 2018 entró en vigor el Reglamento General de Protección de Datos (RGPD)[21] de[22] la Unión Europea para mejorar la protección de los datos personales y al mismo tiempo ampliar los derechos ARCO antes mencionados, trayendo consigo el derecho a la portabilidad de los datos, el derecho al olvido y el derecho de supresión que en definitiva es tener todo el derecho a pedir a las empresas que eliminen nuestros datos, siempre y cuando se basen en nuestro consentimiento.

El RGPD tiene un impacto significativo para las organizaciones y la forma en que manejan los datos, con sanciones potencialmente muy grandes para aquellas empresas que sufren una infracción, llegando hasta el 4% de los ingresos globales.[23]

20. Convenio Europeo de Derechos Humanos, art. 8, 4 de noviembre de 1950, Europ. T.S. nº 5, http://www.echr.coe.int/Documents/Convention_ENG.pdf.

21. El RGPD mejoró y amplió las normas de la Directiva europea sobre privacidad, 95/46/CE, y la Ley Orgánica española 15/1999 de Protección de Datos de Carácter Personal. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML; Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806af30e.

22. Para una comparación de los sistemas regulatorios europeos e interamericanos que rigen la protección de datos personales, véase Francisco Jose Santamaria Ramos, El principio de responsabilidad proactiva: una oportunidad para un mejor cumplimiento de la normativa en materia de protección de datos de carácter personal en el ámbito latinoamericano (F. Santamaria Ramos (2020). El principio de responsabilidad proactiva: una oportunidad para un mejor cumplimiento de la normativa en materia de protección de datos de carácter personal en el ámbito latinoamericano. Derecho PUCP, 85https://go.gale.com/ps/anonymous?id=GALE%7CA648142290&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=02513420&p=IFME&sw=w).

23. GDPR: Lo que necesita saber sobre el Reglamento General de Protección de Datos. https://www. powerdata.es/gdpr-proteccion-datos, Power Data.

Declaración Universal de los Derechos Humanos, la comunidad internacional ha elaborado diversas directrices y principios de buenas prácticas en materia de protección de datos.

Organizaciones intergubernamentales como la OCDE y las Naciones Unidas, así como institutos internacionales de investigación y organizaciones de desarrollo,[26] han contribuido colectivamente a dar forma a los derechos y responsabilidades en materia de protección de datos.

Las Directrices de la OCDE de 1980, actualizadas en 2013, por ejemplo, identifican ocho (8) principios relevantes para la implementación nacional de la protección y uso de la privacidad de los datos: (1) limitación de la recogida; (2) calidad de los datos; (3) especificación de la finalidad; (4) limitación del uso; (5) garantías de seguridad; (6) apertura; (7) participación individual; y (8) responsabilidad.[27] El Grupo de Desarrollo de las Naciones Unidas (UNDG), por su parte, ha recomendado nueve (9) principios de buenas prácticas que sustentan la política de privacidad de datos: (1) uso lícito, legal y justo; (2) especificación de la finalidad, limitación del uso y compatibilidad de la finalidad; (3) mitigación y evaluación del riesgo; (4) datos sensibles y contextos sensibles; (5) seguridad de los datos; (6) conservación y minimización de los datos; (7) calidad de los datos; (8) datos abiertos y transparencia; y (9) diligencia debida para la colaboración de terceros.[28] En su esencia, los principios proporcionan una armonía entre la protección de la privacidad, la transparencia y el intercambio de datos.

Por otra parte, la comunidad internacional señala varios retos para la aplicación de la legislación y las políticas de protección de datos, como las lagunas en la cobertura, las nuevas tecnologías, la transferencia transfronteriza de datos, la vigilancia, la aplicación, la jurisdicción y la carga de cumplimiento para las empresas.[29] Tanto, la legislación y las políticas deben estar siempre atentas a las asociaciones público-privadas, la cooperación y la transparencia.[30]

IV. PROYECTOS DE LEY EN DISCUSIÓN

La Asamblea Legislativa de El Salvador recientemente aprobó la primera ley de protección de datos junto a una ley que crea una autoridad encargada de regir la materia.

26. Véanse, por ejemplo, los principios de privacidad de los datos expuestos por el Banco Mundial (en los que se habla del RGPD como un marco normativo completo que incorpora la mayoría o la totalidad de estos principios). Banco Mundial, Data Protection and Privacy Laws, https://id4d.worldbank.org/guide/data-protection-and-privacy-laws.

27. OCDE, Directrices sobre la protección de la privacidad y los flujos transfronterizos de datos personales (2013), http://www.oecd.org/digital/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

28. Grupo de las Naciones Unidas para el Desarrollo, Data Privacy, Ethics and Protection: Nota de orientación sobre Big Data para la consecución de la Agenda 2030 (2017), https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf.

29. Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, Normas de protección de datos y flujos internacionales de datos: Implicaciones para el comercio y el desarrollo (2016), https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf.

30. Id.

Ley de protección de datos

El debate de la Ley de Protección de Datos comenzó en noviembre de 2019 con consultas a las partes interesadas.[31] El objetivo principal del proyecto de ley era prohibir que se compartan datos sensibles con fines comerciales sin consentimiento.[32] Los datos sensibles para los fines del proyecto de ley incluyen información íntima, como el credo, la religión, el origen étnico, la afiliación política o las ideologías, la afiliación sindical, las preferencias sexuales, la salud física y mental, la información biométrica, la genética y otros. Cabe destacar que lel proyecto de ley no regularía los datos ya regulados por la legislación vigente, como la información crediticia, que ya está regulada por la Ley de Regulación de la Información Crediticia de 2011.

El proyecto de ley también codificaba la protección de cuatro derechos fundamentales sobre los datos, conocidos colectivamente como "ARCO": (A) el acceso a la información ("Acceso"), (R) la corrección de los datos personales (por ejemplo, si uno paga una deuda, la empresa debe actualizar los registros para mostrar que la deuda ha sido pagada) ("Rectificación"), (C) la eliminación de datos antiguos ("Cancelación"), y (O) el derecho a ser olvidado ("Oposición"). La última versión del proyecto de ley fue aprobado por la Comisión Económica, y pasó al Pleno Legislativo para ser discutida y aprobada.

La sociedad civil señaló muchas críticas importantes y significativas sobre el contenido y el proceso de redacción del proyecto de ley.[33] Para algunos, el proceso de redacción del proyecto de ley fue apresurado y no ofreció oportunidades adecuadas para que los legisladores participaran debido a la pandemia de Covid-19. Por lo tanto, los críticos sostienen que el gobierno no ha dado tiempo suficiente para considerar y sopesar las disposiciones del proyecto. El proyecto de ley también establecía excepciones que van más allá de los límites de protección de datos que las leyes anteriores ya habían establecido.[34] Permite excepciones para la seguridad pública o del Estado, sin una notificación adecuada ni definiciones precisas. Esta vaguedad deja un amplio margen por el que estas excepciones podrían ser aprovechadas por las autoridades gubernamentales o las empresas con fines nefastos. La cuestión de la vaguedad continúa en la actual interacción del proyecto de ley; los críticos sostienen que muchos de sus términos clave carecen de claridad o precisión. Por ejemplo, el proyecto de ley señala que los datos deben ser procesados legalmente, sin explicar en qué consiste el procesamiento legal de datos. Este proyecto de ley fue vetado por el presidente de El Salvador.* La eventual aprobación del proyecto de ley requerirá probablemente una importante negociación política para desarrollar un proyecto de ley que sea claro, útil y que proteja significativamente los datos personales de los ciudadanos.

33. Hernandez, Laura. 2021 March 3. "Ley de datos personales: sin pausa, pero sin prisa y de cara a la sociedad." Derechos Digitales. https://www.derechosdigitales.org/15341/ley-de-datos-personales-sin-pausa-pero-sin-prisa-y-de-cara-a-la-sociedad/

34. Velazquez, E. Rodriguez, M. 2021 March 11. "Ley de Protección de Datos prohíbe revelar salud física y mental de las personas." El Salvador. https://www.elsalvador.com/noticias/nacional/ley-proteccion-datos-asamblea-legislativa-prohibe-revelar-salud-fisica-mental/815907/2021/

* Rodríguez, Milton. 2021, Mayo 5 . "Bukele veta Ley de Protección de Datos Personales y otros decretos". https://www.elsalvador.com/noticias/nacional/nayib-bukele-veto-ley-proteccion-datos-personales/839543/2021/

V. RECOMENDACIONES PARA TODOS LOS SECTORES

Gubernamental

El gobierno de El Salvador y su órgano Legislativo deben introducir cambios al proyecto de ley y volver a discutir su contenido de la forma más transparente y participativa posible sin importar los partidos políticos.

Sociedad civil

La sociedad civil debe permanecer vigilante a medida que se acerca la discusión de un nuevo proyecto de ley de protección de datos. Las organizaciones de la sociedad civil han identificado defectos en la legislación, y debe seguir esforzándose para que estas preocupaciones sean escuchadas por el gobierno. Las organizaciones locales de la sociedad civil también deben conectarse con la red más amplia de entidades latinoamericanas de derechos digitales, que pueden ser capaces de proporcionar apoyo, experiencia, perspectiva y comunidad pertinentes a los esfuerzos de protección de datos. Además, la sociedad civil debería considerar las formas en que otros sectores podrían avanzar en sus esfuerzos. Por ejemplo, a medida que el régimen de protección de datos entra en vigor, el estudio de su impacto a través del análisis académico y la teorización jurídica continua ayudará a proporcionar información y recursos útiles para garantizar que los defectos del proyecto de ley no queden intactos.

Otros sectores

Las empresas afectadas por esta legislación, grandes y pequeñas, deben seguir haciendo oír su voz. Cuando las empresas compartan puntos de vista con otras partes interesadas, deberían considerar la posibilidad de colaborar, asegurándose de que las entidades sin ánimo de lucro reciban una compensación por el tiempo dedicado a dicha colaboración. En términos más generales, las empresas deberían comprometerse de forma proactiva con las buenas prácticas de protección de datos, independientemente de la legislación o la política actual, por una serie de razones. En primer lugar, se distinguirá más eficazmente como líderes sociales con una ventaja competitiva sobre las empresas que no cuidan tanto los datos de los consumidores.

En segundo lugar, evitarán futuros riesgos y conflictos que podrían surgir de normas contradictorias o preocupaciones relacionadas con los datos, ahorrando recursos y capital.

VI. CONSEJO PARA QUE EL SALVADOR TENGA SU PROPIA REGULACIÓN

Es importante señalar que las mejores prácticas para la aplicación de un marco normativo eficaz en materia de protección de datos no sólo dependen de las recomendaciones regionales e internacionales, en consonancia con el derecho internacional de los derechos humanos, sino también de las circunstancias y necesidades únicas del país. En otras palabras, las mejores prácticas deben adaptarse a las necesidades específicas del Estado. Dicho esto, varios principios de alto nivel pueden regir en este ámbito.
Sugerencias:

- Acceso: La protección de datos abarca no sólo la protección de la información personal y la privacidad, sino también el suministro de información pública a los individuos. Por lo tanto, de acuerdo con los materiales internacionales comentados anteriormente, un marco político integral de protección de datos promueve y protege necesariamente el acceso a la información pública, el intercambio de datos y el suministro de información sobre los propios datos a las personas.

- Seguridad: La protección de los datos también requiere, en su esencia, una infraestructura que asegure los datos, garantice su calidad y exactitud, y controle su "ciclo de vida", para que ningún imprevisto los vulnere, utilice o manipule.35

- Gobernanza: Una política global de protección de datos se beneficia de un marco de gobernanza que la supervisa, adapta y aplica. Los mecanismos de gobernanza también promueven la responsabilidad ante el público.

- Ejecución: Para reivindicar los derechos individuales, la política de protección de datos debe estar respaldada por un sólido mecanismo de aplicación, que se apoye en los agentes estatales, los tribunales y un marco internacional de derechos humanos subyacente reconocido por la Constitución.

- Colaboración público-privada: Un marco de protección de datos eficaz y completo no termina con la legislación. Más bien, suele incluir un mecanismo administrativo para establecer directrices que puedan adaptarse a las circunstancias cambiantes o a una mejor información; mecanismos de aplicación que sancionen las conductas que violen los derechos de los demás; y asociaciones público-privadas que incentiven el cumplimiento y garanticen la comprensión de las políticas. Especialmente en el ámbito de las plataformas digitales y los intercambios de información, las entidades privadas pueden ser las mejor situadas para aplicar la política de protección de datos y alcanzar los objetivos de la legislación en la materia. Por lo tanto, es imperativo que se les anime a hacerlo.

35. Véase, por ejemplo, GovLab para una definición del ciclo de vida de los datos y la importancia de los mecanismos de gobernanza. https://medium.com/data-stewards-network.

VII. CONCLUSIÓN

El Salvador ha realizado avances envidiables en la construcción de una política pública de protección de datos personales durante los últimos dos años. En mayo de 2021, el Presidente Bukele vetó la ley argumentando falta de presupuesto y experiencia técnica.

Desde IPANDETEC y como actores de sociedad civil defensora de los derechos humanos en el entorno digital centroamericano, apoyamos la promulgación de una ley integral, con enfoque de derechos humanos, discutida abiertamente en concenso con todos los sectores.

IPANDETEC

CENTROAMÉRICA