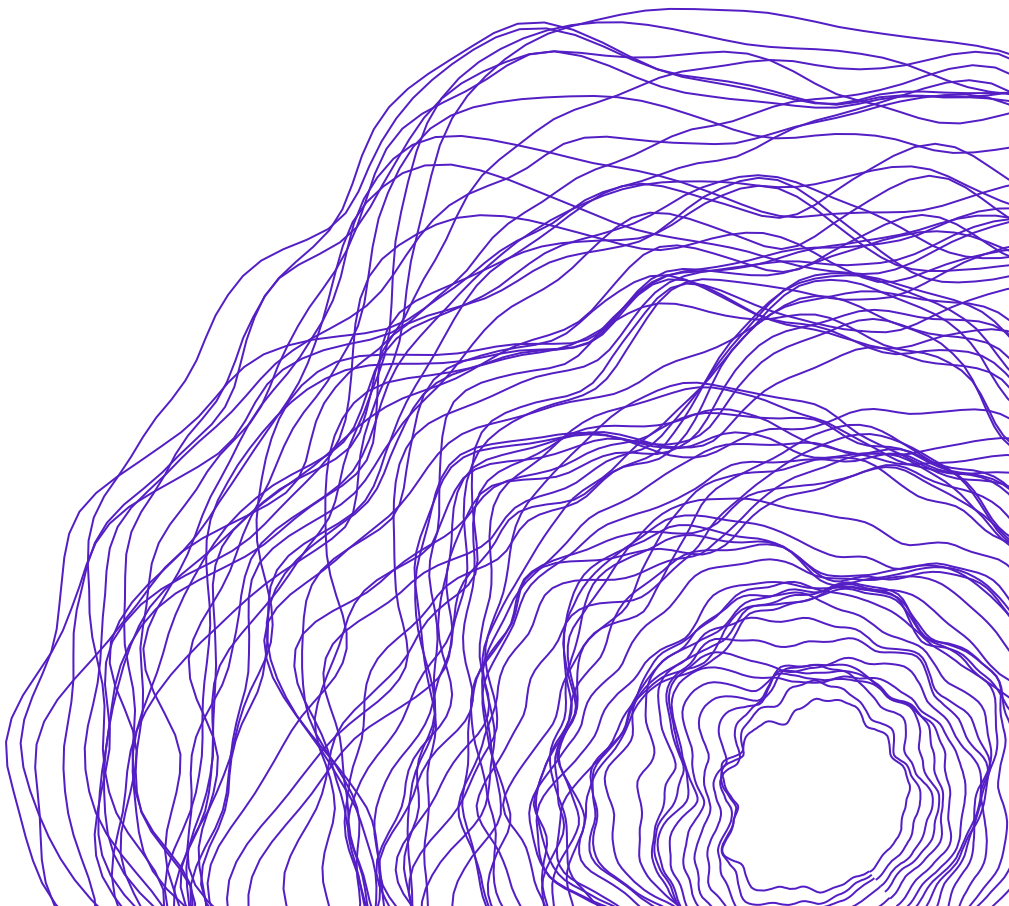
Comprender los Retos a los que se Enfrentan los Reguladores de Protección de Datos: Una Lucha Global hacia la Implementación, Independencia y Cumplimiento

Pawel Popiel y Laura Schwartz-Henderson

Con prólogo de Eduardo Bertoni



Acerca de Este Informe

Desde 2018, más de sesenta países de todo el mundo han promulgado o propuesto nuevas leyes de protección de datos, y esos números aumentan constantemente cada año. Los organismos y agencias reguladores de protección de datos tienen la responsabilidad masiva de hacer cumplir estas leyes recientemente aprobadas en todos los sectores de la sociedad, a menudo con recursos insuficientes, con presupuestos reducidos y un personal escaso. Muchos países siguen lidiando con la cuestión de la independencia, ya que estos órganos suelen estar ubicados dentro de ministerios y oficinas ejecutivas, o están financiados, o conectados con ellos, al tiempo que también tienen la tarea de garantizar que las entidades gubernamentales y los partidos políticos cumplan con la ley.

A finales de 2021, el proyecto ADAPT de Internews reunió a un grupo que representaba a las autoridades reguladoras de protección de datos (APD) en 11 países de África y América Latina para una mesa redonda y discutir los retos que enfrentan al establecer, implementar y hacer cumplir las leyes de protección de datos recién creadas, así como para intercambiar ideas sobre las mejores prácticas y oportunidades de colaboración transfronteriza. Basándose en esta conversación y en entrevistas adicionales con reguladores e informantes clave de la sociedad civil, este informe busca esbozar los retos clave que enfrentan las APD y las áreas de apoyo e intercambio de información.

Los autores agradecen a todos los participantes de la mesa redonda y entrevistas, y destacan en particular los comentarios y contribuciones de Eduardo Bertoni, Rafael Zanatta, Luã Cruz, Khadijah El-Usman, Hlengiwe Dube, Benjamin Whitehead y Skyler Sallick

Índice de Contenidos

Un breve avance desde la perspectiva de una antigua APD

Me complace que se me haya pedido que escriba la introducción a este informe sobre los retos a los que se enfrentan los reguladores de la protección de datos en África y América Latina. El informe se basa en las conversaciones y el debate que iniciamos durante un taller multilingüe al que fui invitado a organizar juntamente con 11 reguladores de África y América Latina. El informe resultante busca extraer algunas de las principales conclusiones de esta conversación, y los autores se basan en los temas discutidos durante este evento, incluidas entrevistas de seguimiento con expertos interesados de ambas regiones. Si bien el siguiente informe describe y cataloga de manera excelente una variedad de problemas que las APD deben enfrentar, como la independencia, el financiamiento, la capacidad técnica y la experiencia, y los desafíos de cumplimiento, pensé que la mejor manera de entrar en una discusión sobre estos desafíos sería contar una historia más personal sobre lo que he presenciado como defensor y regulador en América Latina, y más específicamente en Argentina, donde dirigí la Autoridad de Protección de Datos de 2016 a 2020.

Como mencioné en otro trabajo, en los [1] últimos veinte años, varios países de América Latina han promulgado sus propias leyes de protección de datos y, en muchos casos, estas leyes han seguido las normas que se desarrollaban y se siguen desarrollando en la Unión Europea. A pesar de ello, sólo unos pocos de esos países -a saber, Uruguay, Argentina y México- se han adherido a la Convención 108. Por otra parte, son menos los países -sólo Uruguay y Argentina- a los que se les han otorgado «decisiones de adecuación» que son regularmente determinadas por la Comisión Europea y aprobadas por la Unión Europea.

Los beneficios para quienes obtienen estas decisiones son, entre otros, permitir el libre flujo de datos entre la UE y esos países de acuerdo con la Directiva de Protección de Datos 95/46/CE (en adelante, la "Directiva"). Puede que no sea una coincidencia que dos de los tres países que han ratificado el tratado (Convenio 108) también hayan sido considerados adecuados por la Unión Europea. En este sentido, podría ser importante mencionar que el Convenio 108 y el RGPD, son dos piezas del mismo rompecabezas que ha estado influyendo en muchas de las reformas.

Muchas de las nuevas leyes de protección de datos se inspiraron tanto en el RGPD como en la Convención 108. Sin embargo, aprobar regulaciones que cumplan con estas normas internacionales no ha sido un trabajo fácil. Las normas a menudo no coinciden con la capacidad regulatoria, y las reformas necesarias son muy importantes. Además, hay muchos retos que enfrentar antes de tener leyes que cumplan con los estándares

[1] Eduardo Bertoni, "*Convention 108 and the GDPR: Trends and Perspectives in Latin America*," *Computer Law & Security Review* 40 (abril de 2021): 105516, https://doi.org/10.1016/j.clsr.2020.105516.

internacionales. Por supuesto, muchos de esos retos suelen estar motivados política y económicamente.

La historia de la ley de protección de datos personales argentina demuestra dos de los retos más importantes que enfrentan las autoridades de protección de datos en América Latina y en África. El primer reto se refiere al diseño de la oficina para que sea independiente, tanto en la práctica como en la regulación. El segundo está vinculado a la «fuerza» que tienen las autoridades de protección de datos para hacer cumplir la ley.

En resumen, la historia es la siguiente: Argentina reformó su Constitución en 1994. La reforma introdujo el artículo 43, que establece:

Cualquier persona deberá presentar esta acción para obtener información sobre los datos propios y su finalidad, inscritos en registros públicos o bases de datos, o en privados destinados a suministrar información; y en caso de datos falsos o discriminación, esta acción podrá presentarse para solicitar la supresión, rectificación, confidencialidad o actualización de dichos datos. No se podrá perjudicar el carácter secreto de las fuentes de información periodística.

Poco antes del inicio del siglo XXI, había comenzado en Argentina un fuerte debate para aprobar una ley que regulara concretamente este artículo 43 de la Constitución. Así, en el año 2000, el Congreso aprobó un proyecto de ley de protección de datos personales que incluía dos temas que quiero destacar.

La primera cuestión se refiere al hecho de que el proyecto aprobado por el Congreso incluía la existencia de una oficina específica encargada de controlar el cumplimiento de la ley. Pero, además, la ley designaba quién estaba a cargo de esa oficina -un director nombrado por el presidente y aprobado por el Senado- para garantizar la independencia y la autonomía.

La segunda cuestión se refiere a las multas. Por muchas razones que no están relacionadas con esta conversación, Argentina en ese momento tenía una economía estable donde la equivalencia entre el dólar estadounidense y el peso argentino era de 1US$ = 1AR$. Los políticos de la época estaban convencidos de que la paridad entre el dólar estadounidense y el peso argentino duraría mucho tiempo. Por esa razón, muchas de las leyes que se aprobaron en ese momento -cuando expresaron los montos de las multas- no incluían formas de actualizarlas a lo largo del tiempo. La multa máxima que se incluyó en el proyecto de ley fue de AR$ 100.000.

En Argentina, una vez que un proyecto es aprobado en el Congreso, es enviado al presidente de la Nación para su aprobación o su derecho de veto. El veto puede ser total o parcial. En ese momento -en el año 2000- el presidente de Argentina vetó parcialmente la ley y anuló el artículo que definía el proyecto de la autoridad de protección de datos. De acuerdo con el Decreto Nº 995/2000 firmado por el presidente, el motivo del veto estaba relacionado con cuestiones presupuestarias.

Vetar sólo esa parte del artículo creaba un problema: la ley mencionaba en general la existencia de un organismo que supervisara la nueva ley de protección de datos, pero, debido al veto, la ley no proporcionaba detalles sobre ese organismo de supervisión.

En otras palabras, el resultado del veto era claro: Argentina tiene una ley de protección de datos personales que dice que existe una oficina encargada de hacerla cumplir, pero no describe quién está a cargo de esa oficina, cómo podría ser nombrado o destituido, o dónde se ubicaría esa oficina. Por esa razón, al año siguiente, el presidente, al regular la ley, creó esa oficina, pero como una Dirección dentro del Ministerio de Justicia y Derechos Humanos. El director de la oficina puede ser nombrado o destituido por el ministro de Justicia como cualquier otro empleado.

Por este motivo, la independencia y autonomía de la autoridad de protección de datos se vio muy afectada, lo que suscitó preocupaciones internacionales sobre la independencia real de la recién creada APD. A pesar de esta deficiente regulación, la Argentina argumentó ante la Unión Europea y el Consejo de Europa que la oficina había estado actuando de manera independiente. Esos argumentos tuvieron éxito en ese momento, y se consideró que la Argentina era un país con una legislación adecuada. Para agravar este problema tan agudo con la independencia estructural de la APD, la inflación en Argentina durante los últimos 20 años aumentó sustancialmente. Ya no existe esa paridad entre el peso argentino y el dólar estadounidense. Por lo tanto, la multa máxima que puede imponer hoy la autoridad de protección de datos en Argentina es de apenas quinientos dólares estadounidenses.

Durante muchos años, yo, así como otros expertos y defensores, seguimos argumentando que se necesitaba y exigía urgentemente un cambio en la regulación. Esto finalmente sucedió en 2017. Pudimos cambiar las regulaciones necesarias para incluir la APD en el marco de la entonces recién creada Agencia Nacional de Acceso a la Información, una oficina independiente creada por ley con su propio presupuesto y con la aclaración específica de que el director no podría ser despedido por el presidente sin tener un acuerdo del Congreso.

La historia del derecho argentino y la evolución de la APD, uno de los primeros de la región, deja varias lecciones para todos los países que están proyectando o implementando nuevas leyes.

Las nuevas leyes de protección de datos deben construirse a través de una consulta y consenso significativos entre los diferentes actores (sociedad civil, sector privado, academia, y también algunas oficinas gubernamentales específicas, como los Bancos Centrales, las Oficinas de Impuestos, etc.) para que la autoridad de protección de datos sea independiente y autónoma y para que esto se establezca en la ley. Al proyectar las leyes de protección de datos, no se puede subestimar la importancia de la independencia de las autoridades de protección de datos y es necesario contar con mecanismos claros para el cumplimiento de la ley. Las leyes de protección de datos

deben ser sólidas, pero también flexibles para futuros cambios tecnológicos, políticos y económicos. Las multas también deben ser disuasorias de tal manera que aquellos que son tentados a quebrantar la ley no lo hagan.

Para ser claros: las lecciones aprendidas del caso de Argentina son mucho más que las mencionadas anteriormente, pero no puedo subestimar la importancia de la independencia de la APD, en particular los siguientes puntos clave:

- La independencia de la APD es clave para el éxito de cualquier regulación de protección de datos.
- La independencia debe estar garantizada por la ley.
- La independencia debe ser aceptada en la práctica por las diferentes partes interesadas.
- La independencia también significa dar a las APD suficientes recursos para cumplir con sus deberes.
- La independencia también significa tener un personal con suficiente experiencia para llevar a cabo investigaciones serias.

Pero el trabajo por delante no se detiene con estas muchas cuestiones. Los avances en tecnología son muy rápidos ahora. Además, en esta época, las posibles violaciones de los datos personales situados en un país pueden producirse fuera de las fronteras donde se encuentran las autoridades de protección de datos de esos países. Por lo tanto, es necesario generar mecanismos que permitan a las APD llevar a cabo investigaciones transfronterizas, e incluso imponer sanciones a las empresas no ubicadas en sus territorios. El siguiente informe busca agregar las perspectivas de varios reguladores, expertos y defensores para comprender mejor cómo algunos de estos desafíos se desarrollan en diferentes jurisdicciones. Al final del informe, también hemos destilado algunas de las mejores prácticas sugeridas para las APD individuales, así como para la colaboración entre las agencias reguladoras y las sociedades civiles dentro y entre los países. Esperamos que este informe pueda ser utilizado como una herramienta por defensores, legisladores y reguladores en todas las etapas del proceso legislativo y regulatorio.

Construir leyes y estructuras regulatorias a la altura de la compleja y siempre cambiante tarea de proteger los datos de los ciudadanos no es una tarea fácil. Pero vale la pena intentarlo. La protección de los datos personales está estrechamente relacionada con el derecho humano a la privacidad. Por eso, cuando trabajamos para evitar que se viole un derecho humano, cualquier esfuerzo y creatividad son bienvenidos.

Introducción

Como resultado de la creciente difusión del acceso a Internet en las regiones del Sur Global y la rápida expansión e integración de las economías mundiales de datos, los flujos de datos[2] regionales implican a más usuarios en una creciente gama de actividades diarias. Si bien la participación en estas economías puede permitir una mayor innovación y crecimiento económico junto con otros beneficios potenciales, también introduce daños significativos. Por ejemplo, la expansión de las infraestructuras de datos ha aumentado la capacidad de los proyectos de vigilancia estatal, incluida la acumulación de datos personales de los individuos.[3] Del mismo modo, el uso cada vez mayor de datos por parte de los sectores público y privado plantea mayores preocupaciones en materia de ciberseguridad y plantea cuestiones clave sobre la rendición de cuentas de los controladores y procesadores de datos.[4] La consiguiente y cada vez mayor recopilación de datos por parte de un número creciente de entidades privadas -desde empresas de redes sociales hasta bancos comerciales y agencias de crédito- agrava estas preocupaciones de seguridad, al tiempo que intensifica los riesgos de orientación del comportamiento y de inexactitud de los datos, lo que puede resultar en la prestación discriminatoria de servicios públicos y privados clave.[5]

Los marcos de protección de datos y las agencias reguladoras que los hacen cumplir son mecanismos esenciales para gobernar estos flujos de datos. Sin embargo, a pesar de los considerables progresos realizados en el Sur Global para aplicar esos marcos, persisten los retrasos. En la actualidad, el 71% de los países del mundo cuentan con alguna legislación de protección de datos, incluido el 73% en América Latina, mientras que en África y Asia lo hacen el 61% y el 57%, respectivamente.[6] Dado que la legislación del Reglamento General de Protección de Datos (RGPD) de la Unión Europea ha establecido el estándar global para la regulación de la protección de datos, el hecho de no imponer protecciones igualmente sólidas margina económicamente a los países del Sur Global que carecen de ellas, al tiempo que aumenta los riesgos locales de vigilancia,

[2] UNECLAC, "*Data, Algorithms and Policies*: *Redefining the Digital World*" (Comisión Económica de las Naciones Unidas para América Latina y el Caribe (CEPAL), abril de 2018), https://repositorio.cepal.org/bitstream/handle/11362/43515/7/S1800052_en.pdf; Héctor J. Lehuedé, "*Corporate Governance and Data Protection in Latin America and the Caribbean*" (Santiago: UN Economic Commission for Latin America and the Caribbean (ECLAC), 2019), https://repositorio.cepal.org/bitstream/handle/11362/44629/1/S1900395_en.pdf.

[3] Lukman Adebisi Abdulrauf y Charles Manga Fombad, "*Personal Data Protection in Nigeria*: *Reflections on Opportunities, Options and Challenges to Legal Reforms,*" *Liverpool Law Review* 38, Nº. 2 (2017): 105–34, https://doi.org/10.1007/s10991-016-9189-8.

[4] Ibíd.

[5] Ibíd.

[6] UNCTAD, "*Data Protection and Privacy Legislation Worldwide*", United Nations Conference on Trade and Development (UNCTAD), consultado el 30 de abril de 2022, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

recopilación no consentida y uso indebido de datos.[7] Además, en los países que han aprobado dicha legislación, como en la mayoría de América Latina, los marcos de protección de datos existentes varían en alcance, implementación y nivel de cumplimiento.[8]

La tarea de garantizar el cumplimiento de las leyes de protección de datos, que a menudo requiere educar al sector público y privado sobre los derechos de privacidad y las obligaciones de datos, recae en las Autoridades de Protección de Datos (APD). Estos organismos reguladores -a menudo, aunque no siempre, establecidos con la aprobación de la legislación sobre protección de datos- se enfrentan a una serie de retos en el Sur Global que afectan su capacidad operativa, su capacidad de aplicación y su independencia normativa. Son muchos los factores que contribuyen a estos retos, como la escasez de recursos, la escasa alfabetización digital del público, la inexperiencia de los tribunales y el escepticismo de los responsables políticos.

Para esclarecer y evaluar los factores, este informe examina los retos que enfrentan las APD en África y América Latina. El análisis del informe se basa en los resultados de investigaciones realizadas en dos etapas. La primera etapa consistió en una investigación documental que cotejó el trabajo de expertos, incluidos reguladores de datos, defensores de la protección de datos y académicos sobre la implementación y aplicación de marcos de protección de datos en el Sur Global. Para la segunda etapa, como parte de su proyecto ADAPT (*Advocating for Data Accountability, Protection and Transparency*), Internews convocó una mesa redonda de reguladores de protección de datos de Argentina, Brasil, Burkina Faso, Chile, Mauricio, Marruecos, Níger, Perú, Sudáfrica y Uganda en noviembre de 2021. Esta discusión grabada fue traducida, transcrita y codificada, y sus temas sirven como base para los temas y cuestiones discutidos en este informe. Las conclusiones de la mesa redonda también se complementaron con ocho entrevistas con reguladores actuales y anteriores de la APD, algunos de los cuales participaron en la mesa redonda, así como con representantes de la sociedad civil de ambas regiones. Las respuestas de los participantes en la mesa redonda y en las entrevistas son anónimas en el informe.

Ambas etapas de investigación incluyeron la identificación de retos concretos que enfrentan las APD para implementar y hacer cumplir los marcos de protección de datos, así como las mejores prácticas para abordarlos. Aunque en el informe se destacan en primer plano los retos comunes que enfrentan las APD en África y América Latina, también se destacan las diferencias significativas tanto entre estas dos regiones como dentro de ellas. Sin embargo, a pesar de evaluar los obstáculos poco estudiados para la

[7] Justin Bryant, "*Africa in the Information Age*: *Challenges, Opportunities, and Strategies for Data Protection and Digital Rights,*" *Stanford Law Review* 24 (2021): 389–439; Cara Mannion, "*Data Imperialism*: *The GDPR's Disastrous Impact on Africa's E-Commerce Markets*," *Vanderbilt Law Review* 53, Nº. 2 (2020): 685–711.
[8] DLA Piper, "*DLA Piper Global Data Protection Laws of the World - World Map,*" DATA PROTECTION LAWS OF THE WORLD, 2022, https://www.dlapiperdataprotection.com/index.html.

protección de datos en una muestra de países africanos y latinoamericanos, este informe tiene limitaciones geográficas. Las investigaciones futuras deberían incluir perspectivas de otras regiones para ampliar la relación de los retos únicos y compartidos de las APD en el Sur Global.

Basándose en la investigación documental y los datos cualitativos de las mesas redondas y entrevistas, este informe evalúa los desafíos relacionados con:

1) Creación de una APD
2) Financiación y capacidad de las APD
3) Independencia en la estructura y la toma de decisiones
4) Cumplimiento y sensibilización
5) Aplicación
6) Abordaje de las nuevas cuestiones políticas
7) Colaboración dentro de las regiones y entre ellas con otras APD y con la sociedad civil

Entre ellos, dos factores destacados surgieron como obstáculos clave para una supervisión eficaz de la protección de datos en las dos regiones examinadas en este informe: las limitaciones de recursos y las amenazas a la independencia. Las limitaciones de recursos socavan la capacidad de las APD para despertar la conciencia sobre las leyes de protección de datos, reclutar expertos, realizar investigaciones y llevar a cabo acciones de aplicación, en particular contra las grandes empresas tecnológicas. Las amenazas a la independencia a menudo agravan las limitaciones de recursos, particularmente cuando la organización matriz de una APD o la rama ejecutiva del gobierno controla el presupuesto. También socavan la aplicación efectiva, especialmente del sector público, que se dedica cada vez más a la recopilación y el procesamiento de datos en muchos países de la región.

En el informe también se señalan las mejores prácticas esenciales y se formulan recomendaciones para hacer frente a esos problemas. En particular, los entrevistados destacaron la colaboración entre las APD regionales y entre las APD y la sociedad civil como estrategias especialmente útiles para aumentar la concienciación del sector público y privado, poner en común los recursos, compartir las mejores prácticas, aumentar la experiencia y ayudar en los litigios y aplicación de las normas. Además, estas redes políticas también pueden fomentar la responsabilidad mutua, compensando o reduciendo potencialmente las amenazas a la independencia de las APD. Los entrevistados también señalaron que una prioridad relacionada consiste en reforzar la educación regional para facilitar el cultivo de la experiencia local y la conciencia a nivel comunitario sobre los derechos y las leyes de protección de datos. Dicha experiencia y

familiaridad son esenciales para una aplicación efectiva, un alto cumplimiento de las regulaciones de protección de datos y para convertir las cuestiones de protección de datos en prioridades políticas y sociales.

Retos que enfrentan las APD

Los marcos de protección de datos han proliferado en África y América Latina en la última década. La adopción de estos marcos y el establecimiento de las APD se produjeron en parte en respuesta a las presiones creadas por la aprobación del RGPD y, especialmente en América Latina, el Convenio 108 del tratado internacional de protección de datos del Consejo de Europa (CoE), ratificado por países como Argentina, Cabo Verde y Uruguay.[9] Estos procesos legales y regulatorios también se han visto acelerados por la creciente difusión tecnológica en las dos regiones. Sin embargo, el progreso ha sido desigual y los marcos de protección de datos varían en alcance y robustez. Por ejemplo, en América Latina, Brasil ha liderado la aprobación de la Ley General de Protección de Datos Personales (LGPD) inspirada en el RGPD, mientras que Argentina no ha actualizado su legislación anterior al RGPD.[10] En África, países como Ruanda y Zambia aprobaron su primera legislación de protección de datos en 2021, mientras que Cabo Verde y Burkina Faso actualizaron sus leyes existentes, con la primera superando ciertos requisitos del RGPD.[11] Del mismo modo, países con marcos existentes como Kenia y Sudáfrica emitieron nuevas regulaciones.[12] Sin embargo, muchas leyes en la región no garantizan derechos básicos como la privacidad y otros nuevos como la portabilidad de datos, ni proporcionan medidas clave de rendición de cuentas, como los requisitos para documentar el procesamiento de datos.[13]

---

[9] Eduardo Bertoni, "*Convention 108 and the GDPR: Trends and Perspectives in Latin America*," *Computer Law & Security Review* 40 (abril de 2021): 105516, https://doi.org/10.1016/j.clsr.2020.105516; Council of Europe, "Chart of Signatures and Ratifications of Treaty 108," Council of Europe, 2022, https://www.coe.int/en/web/conventions/full-list; Council of Europe, "Chart of Signatures and Ratifications of Treaty 223," Council of Europe, 2022, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223; Ceyhun Necati Pehlivan, "Editorial: *Data Protection in Latin America*: *An Overview," Global Privacy Law Review 2, no. 2 (2021)*: 102-7.

[10] La introducción de Eduardo Bertoni a este informe discute el marco argentino con más detalle. Véase también, Gilberto Martins de Almeida, "*International*: *A Brief Perspective on Data Protection in Latin America*," *DataGuidance*, enero de 2022, https://www.dataguidance.com/opinion/international-brief-perspective-data-protection; Katitza Rodriguez y Veridiana Alimonti, "*A Look-Back and Ahead on Data Protection in Latin America and Spain,*" *Electronic Frontier Foundation*, 21 de septiembre de 2020, https://www.eff.org/deeplinks/2020/09/look-back-and-ahead-data-protection-latin-america-and-spain.

[11] Aissatou Sylla, "*Recent Developments in African Data Protection Laws – Outlook for 2022*", Hogan Logells Engage, 1 de febrero de 2022, https://www.engage.hoganlovells.com/knowledgeservices/news/recent-developments-in-african-data-protection-laws-outlook-for-2022_1_1.

[12] Ibíd.

[13] Idris Ademuyiwa y Adedeji Adeniran, "*Assessing Digitalization and Data Governance Issues in Africa,*" CIGI Papers No. 244 (Waterloo, Canadá: Centre for International Governance Innovation (CIGI), julio de 2020), https://www.cigionline.org/static/documents/documents/no244_0.pdf.

Aunque la redacción de una legislación sólida y el establecimiento de una APD eficaz son los cimientos de una fuerte protección de datos, los países de África y América Latina se enfrentan o se han enfrentado a una serie de retos en estas etapas iniciales, desde la obtención de apoyo político hasta la garantía de la independencia regulatoria. Una vez establecidas, las APD deben superar las barreras para garantizar el cumplimiento normativo, incluidas las limitaciones significativas de recursos que obstaculizan la aplicación, los mecanismos de sanción limitados y la inexperiencia judicial; la falta de conciencia pública sobre las leyes de privacidad y los derechos y obligaciones de protección de datos; y las intervenciones estatales ocasionales que socavan su independencia y legitimidad regulatoria. Esos obstáculos sirven de contrapunto a la prometedora expansión de los marcos de protección de datos en África y América Latina. Estos obstáculos deben abordarse para maximizar los beneficios de la participación regional en las economías mundiales de datos en términos que reflejen los valores y necesidades locales, al tiempo que se minimizan los daños asociados.

Creación de una Autoridad de Protección de Datos

Los principales retos en el establecimiento de las APD se relacionan con la construcción de apoyo político inicial, la redacción y aprobación de marcos sólidos de protección de datos y la estructuración de la agencia. En primer lugar, los responsables políticos deben elaborar y aprobar una legislación que establezca un marco de protección de datos, y definir la estructura, el mandato y el alcance de la APD que aplicará y hará cumplir este marco. El primer paso en este proceso requiere convencer al gobierno, al público y al sector privado de que una protección de datos sólida debe ser una prioridad política, a menudo en medio de otros objetivos urgentes. Lograr este apoyo representa un desafío clave, particularmente en África, donde se han aprobado menos leyes de protección de datos que en otras regiones y donde persisten importantes brechas en la conciencia pública sobre los problemas de protección de datos.

La elaboración de un marco de protección de datos requiere también el aporte de expertos locales en regulación internacional de protección de datos y en las tecnologías y mercados de uso intensivo de datos para garantizar que dicha legislación no sólo sea exhaustiva, sino que también esté en sintonía con los contextos, necesidades y valores locales. Esta experiencia es especialmente crucial para navegar por la inmensa influencia que los marcos reguladores de la UE ejercen en la protección internacional de datos y para establecer las APD que representen los intereses políticos, económicos y sociales locales. Sin embargo, la escasez de esos expertos, especialmente destacada en África, representa otro reto fundamental para el establecimiento de una APD. A falta de esos conocimientos especializados, la legislación que define la estructura de las APD puede carecer de claridad. Esta falta de claridad organizativa puede dificultar el desarrollo de la capacidad institucional de una nueva APD, en el que los reguladores a menudo deben participar mientras realizan su trabajo normativo diario de cumplir con el mandato de protección de datos. Este doble trabajo, a su vez, puede ejercer una presión considerable

sobre los recursos ya limitados. Además, a falta de tal claridad, las APD pueden enfrentarse a amenazas de la independencia o carecer de mandatos suficientemente amplios para equilibrar la protección de datos con los ámbitos reguladores relacionados, como el acceso a la información, lo que socava la aplicación efectiva. Estos desafíos surgieron como un tema clave en las entrevistas, reflejando las preocupaciones de los reguladores africanos y latinoamericanos.

Aplicación de un marco de protección de datos

Aunque muchos países de África y América Latina garantizan constitucionalmente el derecho a la privacidad,[14] uno de los principales obstáculos para el establecimiento de las APD implica convencer a las élites políticas de que la protección de datos debe ser una prioridad nacional. Esto representa un reto importante, especialmente en África, donde las cuestiones de desarrollo y el crecimiento económico han primado históricamente sobre otras preocupaciones.[15] Al mismo tiempo, los gobiernos ven las leyes de protección de datos con cautela, especialmente si las actividades que ordenan podrían invadir las actividades de vigilancia estatal o ampliar los derechos de acceso público a los datos.[16] En consecuencia, varios marcos de protección de datos de África y América Latina tienen exenciones para categorías a menudo vagas como la seguridad nacional, los servicios de inteligencia y el sector público en general.[17]

El reto de priorizar la protección de datos entre otros objetivos políticos puede verse agravado por la falta de experiencia de los legisladores con la privacidad y la regulación de datos. Entre los principales obstáculos para cultivar esos conocimientos especializados figuran la migración de trabajadores calificados al extranjero o al sector privado, así como la escasez regional de instituciones de enseñanza superior que impartan capacitación en materia de política tecnológica, especialmente en África.[18] La falta de experiencia inhibe la redacción de marcos de protección de datos sólidos, que a

[14] Ademola Adeyoju, "*Internacional*: *Data Privacy Harmonisation in Africa - Progress, Challenges, and Predictions*," DataGuidance, 9 de diciembre de 2020, https://www.dataguidance.com/opinion/international-data-privacy-harmonisation-africa; Rodriguez and Alimonti, "*A Look-Back and Ahead on Data Protection in Latin America and Spain.*"

[15] Alex Boniface Makulilo, "*Privacy and Data Protection in Africa*: *A State of the Art*," *International Data Privacy Law* 2, no. 3 (2012): 163–78, https://doi.org/10.1093/idpl/ips014; Abdulrauf and Fombad, "*Personal Data Protection in Nigeria*."

[16] Abdulrauf and Fombad, "*Personal Data Protection in Nigeria"; Bryant, "Africa in the Information Age*."

[17] Tara Davis, "*Data Protection in Africa*: *A Look at OGP Member Progress*" (Open Government Partnership (OGP), Altadvisory.Africa, agosto de 2021), https://www.opengovpartnership.org/wp-content/uploads/2021/08/OGP-Data-Protection-Report.pdf; Rodriguez and Alimonti, "*A Look-Back and Ahead on Data Protection in Latin America and Spain*"; Abdulrauf and Fombad, "*Personal Data Protection in Nigeria*"; Mpho Ngoepe, "*Balancing and Reconciling the Conflicting Values of Information Access and Personal Data Laws in South Africa*," in *Information Knowledge and Technology for Development in Africa*, ed. D. N. Ocholloa, N. D. Evans, and J. Britz (Cape Town: AOSIS, 2021), 71–84, https://uir.unisa.ac.za/handle/10500/28429; Ewan Sutherland, "*The Governance of Data Protection in South Africa*," *SSRN Electronic Journal*, 2021, https://doi.org/10.2139/ssrn.3922218.

[18] Makulilo, "Privacy and Data Protection in Africa"; Mannion, "Data Imperialism."

menudo establecen las APD y definen su alcance regulatorio. Por ejemplo, los esfuerzos para redactar una legislación en Nigeria, que no tiene un marco legal para la protección de datos, no contaron con la participación de expertos, lo que resultó en casos de «cortar y pegar»,[19] es decir, a la contratación de abogados no especializados que copiaron leyes extranjeras sobre privacidad. Este proceso produjo proyectos de ley débiles o inconsistentes, ninguno de los cuales ha sido aprobado. Además, los responsables de la formulación de políticas no publicaron informes oficiales ni declaraciones públicas sobre la protección de datos, que son cruciales para obtener apoyo para dicha legislación.[20] Los esfuerzos de Sudáfrica para aprobar la Ley de Protección de la Información Personal Nº 4 de 2013 (POPIA), que actualizó el marco de protección de datos del país, siguieron patrones similares: los políticos mostraron poco interés en avanzar en la legislación, cuyo contenido «se extrajo en parte de otros países, con una personalización limitada»[21] y cuya aprobación fue muy lenta. Tales casos contrastan con las redes experimentadas y duraderas de expertos reguladores que los entrevistados describieron en países como Argentina, Brasil, Chile y Colombia, lo que sugiere que la experiencia está distribuida de manera desigual entre África y América Latina.

Como sugieren estas experiencias africanas, en ausencia de experiencia local, los responsables de las políticas que buscan establecer las APD pueden terminar emulando modelos de protección de datos extranjeros, particularmente europeos. Sin embargo, otros factores contribuyen a esa transferencia de políticas. Las regulaciones internacionales de protección de datos a menudo están influenciadas por los marcos del Norte Global, específicamente el RGPD de la UE, que se considera el estándar de oro, y el Convenio 108, particularmente en América Latina. Además de la prominencia reputacional del RGPD, la atracción del importante mercado de la UE significa que es probable que las empresas tecnológicas cumplan con la ley en lugar de renunciar a hacer negocios en Europa. Dado que el RGPD es más estricto que la mayoría de las leyes de privacidad y que se aplica a cualquier empresa que procese los datos de ciudadanos de la UE, existen fuertes incentivos no solo para que las empresas de fuera de la UE lo cumplan, sino también para que los marcos nacionales de protección de datos se armonicen con él. Este «efecto de Bruselas»,[22] a saber, la influencia reguladora internacional de Europa inevitablemente da forma a los marcos de protección de datos en el Sur Global, especialmente porque los costos del incumplimiento, es decir, quedarse fuera de los mercados europeos, tendrá un impacto desproporcionado en los países en desarrollo más pobres.[23]

[19] Abdulrauf y Fombad, "*Personal Data Protection in Nigeria*", 124.
[20] Abdulrauf and Fombad, "*Personal Data Protection in Nigeria*."
[21] Sutherland, "*The Governance of Data Protection in South Africa*", 14.
[22] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (New York, NY: Oxford University Press, 2020).
[23] Mannion, "*Data Imperialism*"; Adeyoju, "*Data Privacy Harmonisation in Africa.*"

Aunque los países de África y América Latina buscan la armonización con el RGPD, especialmente las decisiones de adecuación otorgadas por la UE a los países que cumplen, que facilitan las transferencias de[24]datos transfronterizos, también surgen aquí posibles retos. En primer lugar, las nociones de privacidad difieren entre los contextos políticos y sociales, lo que aumenta el riesgo de incongruencias e incompatibilidades en la traducción de políticas de conceptos como los derechos de los datos. Limitarse a copiar el RGPD para facilitar los flujos de datos transfronterizos puede subyugar los valores y necesidades regionales y locales a los consagrados en el marco de la UE, que centra los intereses en sus ciudadanos.[25] Sin embargo, las prácticas tecnológicas varían. Por ejemplo, los usos de teléfonos inteligentes difieren drásticamente en todo el Sur Global, los límites de la privacidad[26] social pueden ser más borrosos que en Europa, y los conceptos legales clave como «datos personales» e «identidad digital» también tienen diferentes referentes locales.[27] Mientras que la conceptualización occidental reflejada en el RGPD abarca un derecho individualizado a la privacidad, los países del Sur Global pueden priorizar las dimensiones comunales y relacionales de los derechos de privacidad.[28] Además, pueden equilibrar los derechos de privacidad con otros derechos de manera diferente a los países occidentales, por ejemplo, dando prioridad a los derechos al agua o a la atención médica que reflejen los valores y necesidades locales.[29] El hecho de no conciliar los objetivos de protección de datos con las necesidades locales puede intensificar la limitada conciencia pública y el apoyo a la protección de datos que los reguladores observan y denuncian. Por ejemplo, un regulador africano de protección de datos declaró: «todavía escuchas a personas que se preguntan si la privacidad y la protección de datos son importantes». Este organismo regulador señaló que la escasa sensibilización es especialmente prominente en las zonas rurales y entre la población de baja educación, incluida la población analfabeta. Otro regulador africano lo expresó con más franqueza: «Algunas personas piensan que la protección de datos es principalmente para los ricos». Sin embargo, más que una comprensión pública limitada, es probable que tales actitudes también reflejen los desafíos de conciliar los modelos de protección de datos extranjeros con los contextos y necesidades locales. En segundo lugar, el RGPD se construyó sobre 30 años de

[24] Devika Kornbacher et al., "21. *Demonstrating Compliance with Data Privacy Legislation*," LatinLawyer, 3 de agosto de 2021, https://latinlawyer.com/guide/the-guide-corporate-compliance/second-edition/article/21-demonstrating-compliance-data-privacy-legislation.

[25] Bryant, "*Africa in the Information Age*."

[26] Daniel Miller et al., *The Global Smartphone: Beyond a Youth Technology* (UCL Press, 2021), https://doi.org/10.2307/j.ctv1b0fvh1; Seyram Avle, Emmanuel Quartey, and David Hutchful, "*Research on Mobile Phone Data in the Global South*: *Opportunities and Challenges* ", en *The Oxford Handbook of Networked Communication*, por Seyram Avle, Emmanuel Quartey y David Hutchful, ed. Brooke Foucault Welles y Sandra González-Bailón (Oxford University Press, 2020), 487–509, https://doi.org/10.1093/oxfordhb/9780190460518.013.33.

[27] Martins de Almeida, "*Data Protection in Latin America*."

[28] Davis, "*Data Protection in Africa: A Look at OGP Member Progress*"; Martins de Almeida, "*Data Protection in Latin America*"; Makulilo, "*Privacy and Data Protection in Africa.*"

[29] Davis, "*Data Protection in Africa: A Look at OGP Member Progress*."

precedente legal, que muchos países en estas regiones carecen cuando redactan nueva legislación de protección de datos. Por otra parte, la UE dispone de inmensos recursos para aplicar y hacer cumplir su marco, lo que resulta poco práctico para los países en desarrollo que se enfrentan a importantes limitaciones presupuestarias.[30] Finalmente, algunos expertos argumentan que imponer un marco de protección de datos estricto como el RGPD demasiado rápido puede frustrar la innovación local clave para el crecimiento económico regional y la competencia internacional.[31]

Lo que resulta más problemático es que las leyes de protección de datos a veces son financiadas o redactadas por agentes externos con consecuencias preocupantes.[32] Como relató un actor político africano,

> [p]ersonas que no viven en el país, escriben las leyes y el gobierno es entonces [presionado] para aprobar la ley con el fin de acceder a la ayuda o a la ayuda adicional. Muy a menudo esas cosas están vinculadas, y se convierte en un ejercicio de marcar casillas porque la ley está en los libros de estatutos. Cuando se intenta hacerla cumplir o tener algún tipo de mecanismo de aplicación, se percibe que nadie ha recibido un presupuesto para ello.[33]

Además, la imposición externa de leyes de protección de datos y su simple copia puede contribuir a un «efecto de trasplante», es decir, una baja demanda de leyes ajenas a los residentes de una nación, incluso por la percepción de ilegitimidad, lo que da lugar a una mala aplicación.[34] Por lo tanto, los responsables de la formulación de políticas que establecen marcos locales de protección de datos se enfrentan a compensaciones clave entre la armonización de la base de referencia con las normas internacionales, esencial para la previsibilidad regulatoria de las empresas que operan transnacionalmente, por ejemplo, y las expectativas y prioridades locales, que pueden superar los problemas de protección de datos.

Estructuración de una APD

La aprobación de leyes de protección de datos sólidas y legítimas sienta las bases para la eficacia de las APD, pero sigue siendo sólo el primer paso. De hecho, aunque tales leyes a menudo establecen las APD,[35] este no siempre es el caso; por ejemplo, algunos

[30] Michael Pisa and Ugonma Nwankwo, "*Are Current Models of Data Protection Fit for Purpose? Understanding the Consequences for Economic Development*" (Center for Global Development (CGD), agosto de 2021), https://www.cgdev.org/sites/default/files/are-current-models-data-protection-fit-purpose-understanding-consequences-economic.pdf; Mannion, "*Data Imperialism*."
[31] Pisa and Nwankwo, "*Are Current Models of Data Protection Fit for Purpose*?"
[32] Davis, "*Data Protection in Africa: A Look at OGP Member Progress*."
[33] Ibíd., 62.
[34] Bryant, "*Africa in the Information Age*."
[35] Davis, "*Data Protection in Africa: A Look at OGP Member Progress*"; Kornbacher et al., "21. *Demonstrating Compliance with Data Privacy Legislation*"; Lehuedé, "*Corporate Governance and Data Protection in Latin America and the Caribbean*."

países africanos no tienen APD a pesar de tener legislación de protección de datos.[36] Además, la legislación nacional no siempre especifica la estructura de las APD o su mecanismo de financiación, como en el caso de Côte d'Ivoire, Ghana y Malawi.[37] En consecuencia, las APDs varían en edad, estructura organizativa y mandato, entre otras dimensiones.

La falta de claridad legislativa sobre tales factores clave, en particular la estructura y el presupuesto, puede servir como un obstáculo significativo para la función posterior de la agencia. Por ejemplo, varios participantes en la mesa redonda señalaron las consecuencias de la legislación por la que se establecían APD en el seno de otro órgano regulador o en el marco de éste, en lugar de como organismo independiente, en particular la competencia por los recursos, la falta de un mandato claro y las limitaciones a la independencia,[38] como se examina con más detalle en las secciones siguientes del presente informe. Una cuestión estructural conexa destacada por los participantes se refería a si la legislación establecía las APD con un único mandato o con uno doble, que combinara la supervisión de la protección de datos con ámbitos regulatorios conexos como el acceso a la información y la libertad de expresión. Como sostuvo un regulador latinoamericano, las APD de mandato único pueden crear desafíos en la armonización de las leyes que rigen los flujos de información:

> También nos enfrentamos a un reto muy difícil [...] tratando de armonizar la [...] ley general de protección de datos con [...] leyes de acceso a la información pública [...] [E]n caso de que pudiera concentrar los poderes de aplicación en una sola entidad, tal vez esta armonización sería más fácil.

Por el contrario, una APD de doble mandato, como sostuvo un regulador africano, «funciona para nosotros porque el derecho a la privacidad siempre debe equilibrarse con la libertad de expresión y el acceso a la información». Las APD con mandatos duales, como en Argentina y Sudáfrica, tienen un regulador dedicado con autoridad sobre la protección de datos, la transparencia y el acceso a la información. En algunos casos, un regulador de transparencia se encarga de la protección de datos o viceversa, y el orden de ampliación del mandato influye en cómo la APD concilia los objetivos, a menudo en conflicto, entre la protección de datos y la transparencia.[39] Como describió un experto en políticas al redactar la legislación de protección de datos en África, «se empieza con el secreto, ese es exactamente el punto de partida equivocado [dado que] muchos países que ahora tienen estas encantadoras leyes modelo sobre privacidad y protección de datos, tienen leyes impactantes sobre la libertad de medios, libertad de expresión,

[36] Pam Dixon, "*ROUNDTABLE OF AFRICAN DATA PROTECTION AUTHORITIES*: *Status and Response to Privacy Risks in Identity Systems,*" in *ID4AFRICA 5TH ANNUAL CONFERENCE* (Johannesburg, South Africa: *The Round Table of African Data Protection Authorities (RADPA, 2019), 13*, https://www.id4africa.com/2019/files/RADPA2019_Report_Blog_En.pdf.
[37] Davis, "*Data Protection in Africa: A Look at OGP Member Progress*."
[38] véase también Pisa y Nwankwo, "*Are Current Models of Data Protection Fit for Purpose?*"
[39] Lehuedé, "*Corporate Governance and Data Protection in Latin America and the Caribbean*."

acceso a Internet».[40] Dado que la protección de datos puede invadir los flujos de información, lograr el equilibrio adecuado de una manera que refleje los contextos locales es esencial para los marcos efectivos.

Equilibrio entre el crecimiento institucional y la supervisión regulatoria

Una vez establecida legalmente una APD, los reguladores pueden enfrentarse a los retos de equilibrar el trabajo organizativo de establecer la institución reguladora con el trabajo legalmente requerido de supervisión de la protección de datos. Como señaló un actor de la sociedad civil que trabaja estrechamente en la protección de datos en América Latina, los reguladores de APD «realmente no tienen tiempo para establecer su propia institución [...] y seguir [con] su trabajo [que] están legalmente obligados a hacer, que es investigar estos temas, investigar problemas, emitir recomendaciones». Una académica africana y activista de la sociedad civil se hizo eco de estas preocupaciones sobre la APD de su país:

> Están reclutando personal y construyendo una estructura, y esto está sucediendo al mismo tiempo cuando se espera que se pongan en marcha. No hay tiempo para procesar o decir: «Nos estamos construyendo como institución». [...] La protección de datos requiere que estén aplicando o cumpliendo el mandato que les ha sido otorgado por la ley, pero la institución sigue siendo muy inmadura, y el tema de la protección de datos está desarrollándose, está evolucionando.

En el caso de las nuevas APD, la labor de creación de capacidad institucional y de aplicación de la ley suele llevarse a cabo al mismo tiempo. Un regulador africano de datos describió su enfoque para establecer una APD al tiempo que se enfrentaba a la falta de claridad legislativa sobre la estructura organizativa y la capacidad insuficiente:

> Nos nombraron a nosotros cinco sin nada, con un presupuesto de unos US$3,5 millones, y sin personal. Comenzamos literalmente desde cero [...] La parte de protección de datos era bastante difícil. Empezamos haciendo lo que llamamos 'visitas de estudio' a organizaciones similares. Fuimos a Canadá, y fuimos al Reino Unido y a Alemania. Después de eso, los cinco nos sentamos y dijimos: '¿Cómo hacemos entonces esta organización?' Éramos abogados. [...] Como no teníamos dinero, ni siquiera podíamos contratar consultores. [...] Se nos ocurrió la estructura organizativa. [...] Entrevistamos a la gente. Comenzamos por la capa superior que era el CEO y los miembros ejecutivos. [...] Tuvimos que sudar la gota gorda. Ahora tenemos una organización que cuenta con 80 miembros del personal. Ahora tenemos una organización que tiene un presupuesto.

Para las nuevas APD, el trabajo práctico de definir la estructura organizacional, contratar personal, obtener un presupuesto y ampliar la capacidad se lleva a cabo junto con la supervisión de la protección de datos. En consecuencia, las comisiones recientemente

[40] Davis, "*Data Protection in Africa: A Look at OGP Member Progress*," 23.

establecidas a menudo se enfrentan a importantes limitaciones para hacer cumplir los reglamentos y garantizar su cumplimiento. Como señaló un actor de la sociedad civil de África, «no basta con elaborar leyes y decorar nuestros marcos jurídicos con leyes muy bonitas. Es necesario dar un paso más y poner en práctica los principios de protección de datos. Y ahí es donde nos falta bastante». En las secciones siguientes se examinan estos retos con más detalle.

Financiación y capacidad adecuadas

Las limitaciones de financiación son un obstáculo importante para las APD en el Sur Global.[41] Como ejemplo, en 2018 el presupuesto medio de la APD por país africano fue de US$500.000 con 14 empleados y por país latinoamericano fue de US$400.000 con 13 empleados, en comparación con los US$58 millones y 647 empleados por país en América del Norte.[42] Como señaló Teki Akuetteh Falconer, fundador y director ejecutivo de Africa Digital Rights' Hub y antiguo regulador de datos de Ghana, «la cuestión clave no es si los países tienen las leyes 'adecuadas' o las instituciones 'adecuadas' [sino] si tienen los recursos necesarios para aplicar eficazmente las leyes existentes».[43] Aunque los gobiernos del Sur Global dan cada vez más prioridad a la supervisión de la protección de datos, las APD deben competir por la financiación con otras prioridades estatales, como la seguridad nacional y el desarrollo de infraestructura. Como declaró un entrevistado que representaba a una APD africana, el «suministro de recursos del gobierno se centra más en la salud debido al COVID o a esas muchas otras prioridades, como el desarrollo de infraestructura». Entre estos, como destacaron los participantes de la mesa redonda, la pandemia de COVID-19 precipitó importantes restricciones presupuestarias de la APD a medida que los gobiernos reasignaron fondos a los ministerios de salud.

La estructura y el mandato de una APD también influyen en la financiación. Por ejemplo, a pesar de sus beneficios en materia de cumplimiento y armonización, los mandatos duales pueden suponer una carga para los recursos operacionales, como señaló un participante en la mesa redonda. Otro entrevistado de una APD africana argumentó que debido a que su oficina de protección de datos estaba estructurada dentro de otra agencia, «el presupuesto es muy limitado porque [los funcionarios del gobierno] miran nuestro presupuesto en su conjunto. [...] Lo segregarán y dirán que es para la oficina. Pero debido a tantas prioridades en competencia, no tendremos suficientes recursos». Sin embargo, otro encuestado dijo que el hecho de estar enclavado en una organización matriz protegió a su APD de importantes recortes de financiación, especialmente en sus

[41] Bryant, "Africa in the Information Age"; Mannion, "Data Imperialism"; Makulilo, "Privacy and Data Protection in Africa."
[42] Müge Fazlioglu, "*How DPA Budget and Staffing Levels Mirror National Differences in GDP and Population*" (International Association of Privacy Professionals (IAPP), enero de 2018), https://iapp.org/media/pdf/resource_center/DPA-Budget-Staffing-Whitepaper-FINAL.pdf.
[43] Pisa y Nwankwo, "*Are Current Models of Data Protection Fit for Purpose?*", 2.

primeras etapas y durante la pandemia mundial. En muchas jurisdicciones, los problemas de financiación también se ven agravados por la incapacidad de las APD para imponer multas considerables y, a veces, los medios para recaudarlas. Además, las disposiciones legales a veces prohíben a las APD cobrar multas y usarlas para su presupuesto, dirigiéndolas al tesoro en su lugar. En este sentido, algunas APD solo tienen el poder de imponer sanciones penales en lugar de multas administrativas porque, como afirmó un regulador de África, «al gobierno le preocupa que se pueda abusar de este poder».

Los problemas de financiación limitan inevitablemente las actividades de las APD. La insuficiencia de los presupuestos limita las actividades de contratación de personal, lo que afecta a la capacidad de los organismos y a la capacidad de investigación. Un regulador de África que enfrenta limitaciones de recursos explicó que

> en términos de recursos humanos, se está muy limitado. Tenemos una estructura de alrededor de 35 [personal y], en términos de personas con contratos a largo plazo bastante largos, tenemos alrededor de tres. Ahora hemos podido conseguir personal temporal para ayudar [...] pero sus contratos también son muy cortos. Entonces, en cuanto a los recursos humanos, en cuanto a las herramientas, en cuanto a la capacidad de garantizar el cumplimiento, eso es un reto cuando se tienen recursos limitados.

A menudo, al igual que en las agencias reguladoras de Europa y América del Norte, las APD compiten con el sector privado, que cuenta con muchos mejores recursos, por expertos en protección de datos, lo que coloca a las agencias en una situación de desventaja.[44] El fenómeno de la «fuga de cerebros», es decir, la migración de expertos a mercados más lucrativos, a menudo no regionales,[45] intensifica esta desventaja. Además de restringir la capacidad de dotación de personal de las APD, las limitaciones de recursos afectan la capacidad de las agencias para llevar a cabo funciones básicas. Por ejemplo, varios reguladores declararon que el establecimiento de un registro para los controladores y procesadores de datos, clave para mantener la transparencia y la rendición de cuentas, superó las APD con recursos insuficientes y redirigió la atención de la tarea crucial de cumplimiento y monitoreo de cumplimiento. Del mismo modo, las APD recién establecidas y con financiación insuficiente luchan por aumentar la conciencia pública sobre las leyes de protección de datos, que es esencial no solo para establecer el cumplimiento, sino también para la aplicación a través de litigios civiles. Como subrayó un regulador, esas campañas pueden ser costosas, debido a que no sólo deben crearse mensajes públicos, sino que también deben lanzarse repetidamente a través de múltiples canales para garantizar que lleguen al sector público y privado.

[44] Pisa and Nwankwo, "*Are Current Models of Data Protection Fit for Purpose*?"
[45] Mannion, "*Data Imperialism.*"

Garantizar la independencia

La independencia regulatoria de una APD es esencial para su legitimidad, responsabilidad y eficacia.[46] Varios factores interrelacionados dan forma a esta independencia. Los factores estructurales se relacionan con la forma en que se diseña una APD, incluyendo si está situada dentro y es responsable ante otra agencia. Los factores de información se relacionan con la gobernanza de la APD, particularmente con la entidad que supervisa la agencia y si puede anular las decisiones de la APD. Las consideraciones presupuestarias o económicas implican quién controla el presupuesto de una APD, incluidas las preocupaciones sobre la militarización de este control al amenazar con debilitar el financiamiento para hacer cumplir la ley.[47] Juntos, estos factores pueden socavar la independencia institucional y judicial de una APD, y los primeros se relacionan con preocupaciones operativas como la financiación, y los segundos denotan la independencia en la toma de decisiones.[48]

Muchas APD en África y América Latina luchan por lograr la independencia de los actores públicos y privados, lo que socava su capacidad de aplicación. Son especialmente vulnerables a las amenazas a la independencia de los gobiernos que los crean y financian. Las razones oficiales para construir dependencias presupuestarias y de toma de decisiones en la estructura de una APD varían. Por ejemplo, un exregulador latinoamericano de protección de datos señaló que la justificación oficial para estructurar inicialmente la APD del país bajo la égida del Ministerio de Justicia en lugar de como una agencia independiente era que «un nuevo organismo con un presupuesto independiente [...] creará más problemas para el presupuesto nacional [ya que el país] no estaba en una muy buena situación económica y financiera». Esta estructura socavó significativamente la independencia de la APD, y la agencia no fue reformada hasta años más tarde. Del mismo modo, un representante de la sociedad civil ofreció un ejemplo ilustrativo de las amenazas estructurales y financieras a una APD africana:

> Nuestra autoridad reguladora está como fusionada en un ministerio, y ese ministerio está bajo la presidencia. Por lo tanto, no le ha permitido [a la APD] ningún tipo de independencia. No tienen independencia estructural ni independencia financiera. No importa cuán bien intencionada sea la regulación o la legislación, sus manos están constantemente atadas. Los miembros de la junta también forman parte del gobierno. El jefe de la organización es [...] nombrado por el presidente, por lo que realmente no hay espacio para que [los reguladores] pongan el pie en el suelo en términos de cumplimiento, lo que es

[46] Davis, "*Data Protection in Africa: A Look at OGP Member Progress*"; Lehuedé, "*Corporate Governance and Data Protection in Latin America and the Caribbean*"; Internet Society, "*Personal Data Protection Guidelines for Africa*" (Internet Society and the Commission of the African Union, 9 de mayo de 2018), https://www.internetsociety.org/resources/doc/2018/personal-data-protection-guidelines-for-africa/.
[47] Davis, "*Data Protection in Africa: A Look at OGP Member Progress*."
[48] Ibíd., 50.

> un gran problema, porque los mayores procesadores de datos [en el país] son el gobierno.

Incluso los países con sólidos registros de protección de datos se enfrentan a tales limitaciones estructurales. Por ejemplo, la APD de Brasil tiene una independencia limitada del presidente, que tiene control sobre su presupuesto. Además, tres de los cuatro miembros de la junta de la APD son oficiales militares. Estos obstáculos estructurales dificultan las funciones diarias y la capacidad de ejecución de las APD, especialmente cuando el gobierno u otro organismo controlan su presupuesto. Los encuestados también destacaron el papel de los límites de plazo limitados para los reguladores y los procedimientos de reelección no transparentes para socavar la legitimidad y la independencia de las APD. Un regulador latinoamericano enfatizó que factores estructurales como la incapacidad de un APD para modificar la política pública en medio de nuevos desarrollos de protección de datos socavan la independencia judicial.

Dadas las importantes limitaciones de recursos que enfrentan muchas APD, varios participantes de la mesa redonda enfatizaron la importancia de la «independencia económica» o presupuestaria, es decir, la estabilidad y la consistencia financiera. Como declaró un regulador africano, «si no se nos proporciona un presupuesto adecuado, entonces también se vuelve muy difícil para nosotros mostrar realmente nuestra independencia». Sin embargo, muchos participantes vieron que los fondos de la APD fueron reasignados o recortados por los gobiernos durante la pandemia de COVID-19, a medida que proliferaba el trabajo remoto, lo que aumentó la probabilidad de abusos en la protección de datos. Del mismo modo, si bien algunos participantes señalaron que el hecho de estar integrado en otro órgano regulador puede proteger una APD contra las amenazas a su presupuesto, otros observaron lo contrario, incluidas las limitaciones de financiación impuestas por la agencia matriz.

Las limitaciones a la independencia de la APD en África y América Latina se deben no solo a la escasez de recursos, sino también a que la regulación de la protección de datos puede afectar a la actividad del sector público. Como Kuda Hove de Privacy International señaló sobre ciertos gobiernos en África:

> Existe esa desconfianza generalizada en tener instituciones independientes [...] Existe esa desconfianza [de que] si les concedemos una verdadera autonomía, si les damos una verdadera independencia, podrían volverse contra nosotros en el futuro, ese es el sentimiento que tienen los gobiernos. Entonces, para manejar ese miedo, los gobiernos entonces socavarán la independencia.[49]

Por ejemplo, un investigador observó que en Sudáfrica la creación de «agencias independientes nunca ha resultado atractiva para los ministros del ANC [partido

[49] Ibíd.

mayoritario], que prefieren mantener el control», lo que[50] resulta en una lenta implementación de la legislación de protección de datos y su evaluación. Además, la legislación de protección de datos a menudo otorga a los ministros el poder de crear exenciones legales, revisar regulaciones e intervenir en actividades de cumplimiento, haciendo que las APD sean vulnerables a la captura normativa.[51] Por ejemplo, el NDPR (Reglamento de Protección de Datos de Nigeria) de Nigeria puede ser derogado por cualquier ley del Parlamento, y el organismo regulador del país, NITDA (Agencia Nacional de Desarrollo de Tecnología de la Información) tiene un mandato significativamente limitado, incluida la falta de poder discrecional de aplicación.[52] Del mismo modo, la mayoría de las leyes de protección de datos de los países latinoamericanos eximen a las fuerzas del orden y las agencias de inteligencia estatales, como Brasil, Perú y Panamá.[53]

Sin embargo, los actores del sector público se encuentran entre los abusadores prolíficos de la protección de datos personales.[54] Por ejemplo, los funcionarios electorales kenianos presuntamente recopilaron y utilizaron indebidamente datos biométricos durante las elecciones de 2017.[55] Del mismo modo, varias agencias nigerianas recopilaron grandes cantidades de datos públicos como condición para la emisión de documentos estatales clave, como licencias de conducir y pasaportes. Casos similares de violaciones deliberadas o accidentales de la privacidad han surgido en países como Ghana y Sudáfrica.[56] En América Latina, un regulador de datos informó que «el gobierno federal [está] utilizando la ley general de protección de datos [del país] para negar el acceso a la información». Mientras tanto, otros gobiernos de la región se han eximido de las leyes de protección de datos en sus actividades de procesamiento y manejo de datos, incluidas las aplicaciones de rastreo de contactos.[57] Como dijo un representante de la sociedad civil:

> Sabemos que todo lo que ocurre en el sector público, específicamente lo relacionado con el poder ejecutivo, se va a hacer aún más difícil de investigar, o va a haber una investigación superficial. [...] Por ejemplo, el poder ejecutivo y la policía federal están tratando de comprar sistemas biométricos. Y nosotros en nuestra coalición de otras organizaciones denunciamos eso, y [...] las autoridades dijeron: 'No, está todo bien, puede contar con nosotros.'

[50] Sutherland, "*The Governance of Data Protection in South Africa*", 14.
[51] Ademuyiwa y Adeniran, "*Assessing Digitalization and Data Governance Issues in Africa*."
[52] Bryant, "*Africa in the Information Age*."
[53] Rodriguez y Alimonti, "*A Look-Back and Ahead on Data Protection in Latin America and Spain*."
[54] Bryant, "*Africa in the Information Age*."
[55] Ibíd.
[56] Ibíd.
[57] Javier Pallero, "*Collective Challenges and Opportunities in Data Protection: A Latin American Perspective*", Luminate, 26 de mayo de 2021, https://luminategroup.com/posts/blog/collective-challenges-and-opportunities-in-data-protection-a-latin-american-perspective.

Otro representante de América Latina sostuvo que esta falta de independencia a menudo entrañaba procedimientos regulatorios no transparentes. El entrevistado señaló que, debido a la proximidad del gobierno en cuestión con el sector privado, los funcionarios de la APD a veces se reúnen con una empresa investigada pero no animan a los miembros de la sociedad civil y mantienen los procedimientos ocultos al público. Los representantes de la sociedad civil declararon que a menudo no podían obtener una respuesta de los reguladores, programar reuniones con ellos o acceder a documentos legales relevantes para las investigaciones. Esta opacidad procedimental, a su vez, dificulta la identificación de si una APD no lleva a cabo una investigación concreta por falta de recursos o por intereses y alianzas políticas contrapuestas. En consecuencia, incluso si a menudo se originan en el propio gobierno, las amenazas a la independencia de las APD también pueden afectar las investigaciones en el sector privado.

Cumplimiento y sensibilización

La aplicación y el cumplimiento de las leyes de protección de datos presupone cierto grado de alfabetización digital pública, por ejemplo, para obtener el consentimiento informado de los usuarios antes de la recopilación de datos.[58] Del mismo modo, el cumplimiento de la ley por parte del sector privado requiere que las empresas estén familiarizadas con las leyes y reglamentos vigentes. Ambas condiciones presentan desafíos para las APD, particularmente en países con baja alfabetización digital y difusión tecnológica. Aunque la conciencia sobre los problemas de privacidad ha aumentado en los últimos años, por ejemplo, como lo demuestra un aumento del 20-30 por ciento en las quejas de privacidad presentadas ante las APD africanas,[59]el problema persiste entre la población en general. Por ejemplo, las encuestas realizadas en Ghana revelaron que los usuarios de Internet no estaban familiarizados con las cuestiones de privacidad y protección de datos, y a menudo desconocían sus respectivos derechos de privacidad o qué hacer si éstos eran violados.[60] La investigación también encontró que para muchas personas, la privacidad no era una prioridad.[61] Como dijo un participante de la mesa redonda, uno de los principales desafíos es «la falta de conocimiento [de ambos] en términos de que los interesados conozcan sus derechos e incluso que los responsables del tratamiento conozcan sus obligaciones.» Otros participantes afirmaron que la sensibilización es una prioridad importante para las APD de África y América Latina.

Informar al público sobre la privacidad y la protección de datos es esencial para que las APD puedan cumplir eficazmente sus mandatos. El desconocimiento público de las leyes de privacidad socava no solo la posible aplicación de la responsabilidad civil, sino

[58] Pisa and Nwankwo, "*Are Current Models of Data Protection Fit for Purpose*?"
[59] Dixon, "*ROUNDTABLE OF AFRICAN DATA PROTECTION AUTHORITIES*: *Status and Response to Privacy Risks in Identity Systems.*"
[60] Bryant, "*Africa in the Information Age*."
[61] Ibíd.

también el ejercicio por parte de los ciudadanos de derechos básicos, como los derechos de acceso, corrección o eliminación de los datos personales.[62] Además, la baja alfabetización digital combinada con una conciencia limitada de la privacidad puede socavar los esfuerzos de las APD para aumentar la transparencia en torno a las cuestiones de protección de datos (por ejemplo, mediante el desarrollo de un registro público de datos), y la legitimidad pública de las agencias. A menudo, como señaló un entrevistado de África, las leyes de protección de datos deben traducirse del inglés al idioma local y simplificarse «para que la población pueda entender» '¿Qué gano yo? ¿Cuáles son los beneficios de tener mis datos personales protegidos?'» El entrevistado hizo hincapié en que la creación de conciencia pública es un proceso a largo plazo, a menudo con un uso intensivo de recursos:

> [L]os recursos para llenar las brechas de recursos humanos y luego los recursos en la creación de conciencia son muy importantes. Porque mi punto de vista es que para poder llegar a esta población [que carece del conocimiento de las leyes de protección de datos], hay que enviar este mensaje varias veces, casi todas las semanas, o con frecuencia. Y este espacio mediático requiere tiempo. Se necesita que la gente desarrolle ese contenido. Se necesita pagar para que su mensaje sea transmitido.

En consecuencia, las limitaciones de recursos pueden socavar los esfuerzos para aumentar la conciencia pública de las leyes de protección de datos, lo que a su vez puede intensificar los retos relacionados con la aplicación y el cumplimiento de la APD.

Del mismo modo, tanto los procesadores de datos como los controladores del sector público y privado no están familiarizados con las leyes locales de protección de datos, lo que puede deprimir el cumplimiento y desbordar los esfuerzos de cumplimiento. Por ejemplo, a pesar de la aprobación de la legislación de protección de datos de Sudáfrica en 2013, muchas empresas nacionales y extranjeras siguen incumpliendo y es probable que no se denuncien todas las violaciones de datos.[63] Esta tasa de incumplimiento ha aumentado con la difusión de tecnologías de uso intensivo de datos, como los teléfonos inteligentes.[64] Además, a pesar de años para cumplir con la nueva ley, la investigación revela que solo el 25 por ciento de los sitios web más populares del país piden el consentimiento de los usuarios para recopilar sus datos.[65] Del mismo modo, los investigadores descubrieron que ciertos sitios web del gobierno electrónico de Ruanda no cumplían con los principios básicos de protección de datos, como tener una política de privacidad.[66] Un operador de un sitio web creía erróneamente que la protección de

[62] Davis, "*Data Protection in Africa: A Look at OGP Member Progress*."
[63] Sutherland, "*The Governance of Data Protection in South Africa*."
[64] Ibíd.
[65] Bryant, "*Africa in the Information Age*."
[66] Chantal Mutimukwe, Ella Kolkowska y Åke Grönlund, "I*nformation Privacy Practices in E-Government in an African Least Developing Country, Rwanda*", *The Electronic Journal of Information Systems in Developing Countries* 85, no. 2 (2019): 1–21, https://doi.org/10.1002/isd2.12074.

datos se basa en la legislación fiscal, mientras que otro afirmaba que «no hay ninguna política que seguir; yo [manejo la información personal] siguiendo mi sentido común».[67] El sector público no es inmune al bajo cumplimiento y, en algunos casos, es un delincuente aún peor que el sector privado. Después de exigir que los controladores de datos se inscriban en un registro público recién establecido, un regulador africano de protección de datos observó:

> Hemos observado que, por ejemplo, el sector financiero, es muy cumplidor. Los sectores de seguros son muy cumplidores. Estamos viendo hospitales y clínicas que empiezan a registrarse. Así que eso está mejorando, pero donde hemos notado bajas tasas de cumplimiento es dentro del gobierno. Y esto puede deberse a que no son conscientes de las leyes.

Como resultado, los controladores y procesadores de datos del sector público pueden presentar los mayores desafíos para el cumplimiento y una prioridad clave para las campañas de sensibilización de las APD en torno a las leyes de protección de datos.

Aplicación

Aunque es una de sus responsabilidades más fundamentales, muchas APD en África y América Latina enfrentan retos significativos para hacer cumplir efectivamente las leyes de protección de datos. Éstas se derivan en parte de mandatos de aplicación poco claros y excesivamente estrechos y de exenciones jurídicas ambiguas.[68] Por ejemplo, la APD de Nigeria, la NITDA, carece de un poder de ejecución claro.[69] Otro obstáculo acuciante, y un tema clave en la mesa redonda, es la falta de personal experto y de financiación para perseguir los casos e investigar los abusos. Al mismo tiempo, evaluar las actividades de aplicación de las APD es difícil debido a los datos inconsistentes sobre las investigaciones en todas las jurisdicciones. Por ejemplo, muchas APD africanas no dan publicidad a sus medidas coercitivas, aunque países como Sudáfrica y Ghana han perseguido activamente a las empresas que no cumplen sus obligaciones, y esta última instituyó un tribunal de vía rápida para enjuiciar a los infractores.[70]

Tres desafíos relacionados con la aplicación de la ley implican medidas punitivas. En primer lugar, muchos tribunales africanos carecen de experiencia judicial en materia de protección de datos, a lo que se suma una jurisprudencia insuficiente en materia de privacidad en la región.[71] Los tribunales sin experiencia pueden socavar la ejecución, en

[67] Ibíd., 8.
[68] Davis, "*Data Protection in Africa: A Look Back and Ahead on Data Protection in Latin America and Spain*"; Ngoepe, "*Balancing and Reconciling the Conflicting Values of Information Access and Personal Data Laws in South Africa*"; Pisa y Nwankwo, "*Are Current Models of Data Protection Fit for Purpose?*"; Sutherland, "*The Governance of Data Protection in South Africa*."
[69] Bryant, "*Africa in the Information Age*."
[70] Ademuyiwa y Adeniran, "*Assessing Digitalization and Data Governance Issues in Africa*."
[71] Davis, "*Data Protection in Africa: A Look at OGP Member Progress*."

particular las acciones de responsabilidad civil.[72] Por el contrario, como se ha documentado en Nigeria, cuando el público no está familiarizado con los derechos de privacidad locales, las personas rara vez entablan acciones legales contra los infractores, lo que da a los tribunales pocas oportunidades de desarrollar conocimientos especializados y jurisprudencia sobre protección de datos.[73] En relación con ello, muchos tribunales africanos sufren retrasos importantes y desconfianza pública, lo cual contribuye a la reticencia de las personas a buscar recursos jurídicos.[74] Para las APD que pueden imponer solo sanciones penales en lugar de financieras, un sistema judicial abrumado puede frustrar la aplicación. Como señaló un regulador africano, si bien los gobiernos pueden ser reacios a permitir que las APD dicten multas administrativas debido a la preocupación por el abuso de poder, la alternativa a menudo se retrasa o no se hace cumplir.

En segundo lugar, para las APD que pueden perseguirlos, las sanciones administrativas para los infractores varían ampliamente entre jurisdicciones. Por ejemplo, bajo la ley LGPD de Brasil, las multas pueden oscilar hasta el diez por ciento del bruto anual de una empresa,[75] mientras que en Ghana la multa más alta es de aproximadamente US$10.500.[76] Como mecanismo de disuasión, muchas sanciones se consideran insuficientes.[77] Las medidas coercitivas limitadas, sumadas a la ineficacia de las sanciones, corren el riesgo de cultivar una cultura de impunidad.[78] Estas pequeñas multas son especialmente infructuosas para castigar a las grandes empresas extranjeras infractoras.

Por lo tanto, un tercer desafío relacionado con la aplicación implica perseguir casos contra empresas tecnológicas extranjeras, a menudo grandes. Mientras que los marcos de privacidad europeos y norteamericanos suelen ofrecer protección a los flujos de datos transfronterizos que implican a sus ciudadanos, las grandes empresas tecnológicas de países como Estados Unidos y China recogen y procesan datos de muchos países del Sur Global, a menudo con impunidad.[79] Un estudio reveló que las filiales de las empresas europeas de telecomunicaciones que operan en Senegal y Kenia no ofrecían a los africanos los mismos derechos en materia de datos que sus empresas

[72] Ibíd.
[73] Abdulrauf and Fombad, "*Personal Data Protection in Nigeria*."
[74] Mannion, "*Data Imperialism.*"
[75] Lehuedé, "*Corporate Governance and Data Protection in Latin America and the Caribbean,*" 39.
[76] Ademuyiwa y Adeniran, "*Assessing Digitalization and Data Governance Issues in Africa*."
[77] Ibíd.; Davis, "*Data Protection in Africa*: *A Look at OGP Member Progress*."
[78] Davis, "*Data Protection in Africa: A Look at OGP Member Progress*."
[79] Huw Roberts, Kirra Evans y Charlotte Lenz, "*Data Extraction by Chinese Phone Applications in Africa*: *An Analysis of Risks and Regulatory Protection* ", Oxford China International Consultancy, 6 de mayo de 2021, https://ocicoxford.com/wp-content/uploads/2021/05/Apps-Report-Final-6-May-2.pdf; Sutherland, "*The Governance of Data Protection in South Africa*"; Reuters, "*South African Regulator Seeking Legal Advice on WhatsApp 's New Privacy Policy* ", *Reuters*, 13 de mayo de 2021, sec. África, https://www.reuters.com/world/africa/south-african-regulator-seeking-legal-advice-whatsapps-new-privacy-policy-2021-05-13/.

matrices conceden a los europeos.[80] Como dijo un participante de la mesa redonda, «cuando vamos contra grandes empresas que no tienen su sede en nuestros países, es difícil hacer la investigación, y al final, es difícil hacer cumplir la decisión». Otro entrevistado de América Latina destacó cómo la falta de cumplimiento de las leyes locales, combinada con mecanismos de sanción insuficientes, socavó las acciones de aplicación contra las grandes empresas tecnológicas:

> Si decido un caso contra Google, por ejemplo, la respuesta habitual de Google es: «Sus leyes no se me aplican». [...] E incluso cuando el tribunal dice: «Sí, esta ley se le aplica, tiene que pagar la multa», o lo que sea, a veces es complicado hacer cumplir las decisiones. [...] El otro problema es [...] el monto de las multas es muy bajo cuando se traducen en dólares ahora mismo [...] Es más barato pagar la multa si quieren pagar que, ya sabe, hacer los cambios estructurales que tienen que hacer para respetar la ley.

El desafío de hacer cumplir las leyes locales de protección de datos contra violaciones extranjeras plantea preocupaciones sobre la legitimidad internacional de las APD. Además, como estas acciones de aplicación suelen fracasar, las APD suelen centrarse en las empresas nacionales,[81] lo que puede frustrar la innovación local y socavar la competitividad internacional de las empresas tecnológicas locales.

Además de los obstáculos relacionados con las sanciones, una preocupación acuciante es la falta regional de consultores técnicos expertos. El reto afecta tanto a África como a América Latina y puede complicar las medidas de aplicación. Como dijo un exregulador latinoamericano:

> Si realmente quiere investigar seriamente [una] filtración de datos, necesita buenos informáticos o ingenieros que puedan ir a los registros y ver exactamente si respetaban las salvaguardias básicas para proteger los datos personales o no. Esto es algo que, si usted es un abogado, es muy difícil de entender o de hacer. Por lo tanto, se necesita un departamento específico, un grupo específico de personas, investigadores, que sean técnicos. Y esto es un problema porque en América Latina, y también en Europa por lo que sé, es muy complicado contratar personal de calidad debido al salario de los técnicos, de la gente que trabaja en informática, en seguridad de redes. En este tipo de cosas, por lo general [...] las personas están muy bien pagadas, y no quieren pasarse a una Autoridad de Protección de Datos. [...] Por supuesto, si su presupuesto es bajo, el problema es mucho peor. Desde luego, si no tiene su propio presupuesto, el problema es mucho peor. Pero incluso cuando se tiene un presupuesto, es un problema.

[80] Bryant, "*Africa in the Information Age*", 424; Internet Without Borders, "*Digital Rights in Sub Saharan Africa*: *Analysis of the Practices of Orange in Senegal and Safaricom in Kenya*" (Internet sin fronteras, enero de 2018), https://www.accessnow.org/cms/assets/uploads/2018/02/RDR-Africa_Final-version-5_January-2018.pdf.
[81] Pisa and Nwankwo, "*Are Current Models of Data Protection Fit for Purpose*?"

La falta de recursos y la reducción de los sueldos del sector público obstaculizan la contratación de expertos locales y, cuando se combinan con tribunales inexpertos, pueden dificultar la realización de investigaciones exhaustivas y la imposición de sanciones disuasorias.

Por último, las amenazas a la independencia de la APD también pueden socavar su aplicación. Un defensor de la sociedad civil africana señaló que el gobierno del país no quiere que la APD persiga casos contra el sector público. En consecuencia,

> hasta ahora, todos los esfuerzos [de aplicación] se han dirigido a las empresas. Incluso así, yo no lo llamaría muy eficaz. [Desde la creación de la autoridad unos años antes] ha habido dos o tres procesamientos y no hay manera de que sea una [cantidad] exacta de cuántas personas están infringiendo las leyes de protección de datos.

En última instancia, esta supervisión fragmentaria de la protección de datos erosiona la legitimidad de una APD y, por extensión, su capacidad para cultivar el conocimiento público y privado de los derechos y responsabilidades en materia de datos.

Nuevas cuestiones políticas

Los sistemas tecnológicos establecidos, pero que proliferan como el Internet de las Cosas (IoT), la creciente adopción de tecnologías *blockchain* y computación descentralizada, y los avances en Inteligencia Artificial (IA) conllevan implicaciones para la protección de datos y la regulación de la privacidad.[82] Por ejemplo, los requisitos de eliminación modelados según el RGPD son anteriores y no se pueden aplicar fácilmente a los libros de contabilidad inmutables que caracterizan a las *blockchains*.[83] Los sistemas de IA siguen prácticamente sin regularse en varios países africanos,[84] y los esfuerzos de los encargados de formular políticas para evaluar los enfoques regulatorios de las tecnologías emergentes han sido lentos.[85]

La proliferación de teléfonos inteligentes, IoT y procesamiento en la nube complican significativamente los flujos de datos transfronterizos, lo que plantea preguntas legales clave sobre la obtención del consentimiento y sobre cómo lograr la armonización regulatoria en medio de las diversas reglas nacionales de protección de datos que implican estos flujos de datos.[86] Pocos países africanos tienen normas claras sobre estas corrientes,[87] cuya definición será cada vez más apremiante. Sin embargo, los discursos políticos que simplemente asumen la utilidad social y los beneficios económicos de las

[82] UNECLAC, "*Data, Algorithms, and Policies*."
[83] Bryant, "*Africa in the Information Age*."
[84] Ibíd.
[85] Sutherland, "*The Governance of Data Protection in South Africa*."
[86] Ibíd.; Lehuedé, "*Corporate Governance and Data Protection in Latin America and the Caribbean*."
[87] Pisa and Nwankwo, "*Are Current Models of Data Protection Fit for Purpose*?"

tecnologías emergentes sirven como un obstáculo para el desarrollo de tales reglas. Como destacó un defensor de la sociedad civil africana:

> Parecemos tener una tendencia a abrazar las tecnologías [...] por la conveniencia que traen. Y en la mayoría de los casos, el mensaje sobre la conveniencia del tipo de tecnología anula las preocupaciones relacionadas con la privacidad. En este momento, hay una conversación en torno a la Cuarta Revolución Industrial, ya saben, 'Necesitamos ser parte del mundo desarrollado', 'Necesitamos adoptar esta tecnología.' Pero la conversación sobre la protección de datos de privacidad se pierde por el camino. [...] Y [nuestro país] está avanzando hacia la adopción de un sistema de identificación biométrica más avanzado y centralizado. Y va a ser muy fácil acceder a la información sobre un individuo y todo eso, pero ¿dónde está la conversación en torno a la protección de esa información, esa información tan sensible?

Además, como varios entrevistados señalaron, muchas APD en la región necesariamente priorizan el desarrollo de capacidades, ocupando la mayor parte del enfoque y tiempo de los reguladores de protección de datos. Sin embargo, como señaló un regulador, algunas APD africanas están adoptando enfoques proactivos y desarrollando nuevos marcos de políticas, como las tecnologías impulsadas por la IA y la tecnología financiera.

En América Latina, el desarrollo de regulaciones para las tecnologías emergentes también es desigual. Algunos países se han centrado en la elaboración de marcos para las Nuevas cuestiones políticas. Por ejemplo, Barbados y El Salvador han adoptado tecnologías como las criptomonedas como parte de su plan nacional de desarrollo.[88] Sin embargo, siguen surgiendo nuevas preocupaciones en materia de políticas, en particular en torno a la regulación de los sistemas de identidad digital[89] y la digitalización de los datos de ADN de las personas.[90] Las APD deberán definir la supervisión de estas actividades de uso intensivo de datos. Además, como argumentaron los actores de la sociedad civil de la región, la aplicación existente aún no ha frenado los problemas familiares como las filtraciones de datos, el fraude bancario, las preocupaciones relacionadas con la ciberseguridad en torno a los sistemas de tarjetas de crédito, así como la supervisión insuficiente de las nuevas tecnologías de IA. Como argumentó un representante de la sociedad civil, «la tendencia es que [estos problemas] se hagan más grandes ya que realmente no se está haciendo nada sistemáticamente para lidiar con ello». La incierta realidad política a la que se enfrentan varios países de la región, como afirmaron diversos entrevistados, no hace más que agravar los problemas de capacidad

[88] Martins de Almeida, "*Data Protection in Latin America*."
[89] Ibíd.
[90] Sutherland, "*The Governance of Data Protection in South Africa*."

de las APD a la hora de supervisar las nuevas tecnologías y los consiguientes problemas de protección de datos.

Colaboración con otras APD, Agencias Reguladoras y Sociedad Civil

La colaboración entre las APD regionales, con otras instituciones reguladoras nacionales y con la sociedad civil puede aumentar la capacidad y la eficacia de las actividades diarias de las APD, desde la sensibilización hasta la realización de investigaciones eficientes y exhaustivas. Una mayor colaboración y coordinación regional entre las APD, especialmente útil para las agencias de reciente creación, puede permitir el intercambio de mejores prácticas y reforzar las acciones de aplicación contra las empresas que operan a nivel transnacional.[91] La asociación con otros organismos reguladores nacionales, como las agencias de protección del consumidor y los reguladores sectoriales, puede mejorar las investigaciones de aplicación y aumentar el cumplimiento. Trabajar con la sociedad civil puede cultivar la conciencia pública sobre los problemas de protección de datos, aumentar la responsabilidad y legitimidad de las APD y ayudar a identificar violaciones. A pesar de los inmensos beneficios, estas alianzas también se enfrentan a desafíos, la mayoría de las veces relacionados con objetivos y mandatos divergentes y diferencias culturales ocasionales.

Colaboración con otras APD

La colaboración regional entre las APD ha sido decisiva para la creación de nuevas agencias y el desarrollo de sus capacidades. Por ejemplo, una participante de una mesa redonda de África relató cómo ella y su equipo visitaron agencias de protección de datos en varios países del Norte Global para desarrollar un plan para la APD en su país de origen. Sin embargo, otro entrevistado declaró que las asociaciones con las APD de Global North son muy raras. En cambio, la colaboración es más frecuente a nivel regional, donde compartir las mejores prácticas es igualmente útil, si no más. Un regulador africano relacionó varias formas en que tales colaboraciones refuerzan la protección de datos nacionales:

> Cuando hablo con mi homólogo sudafricano, sí, les ha llevado tiempo llegar a donde están, pero ahora están totalmente financiados. Sus niveles de cumplimiento están aumentando. Entonces, discutiremos, ¿cómo lo han hecho? ¿Podemos obtener ciertos consejos que nos puedan dar? Compartimos marcos como sus documentos estratégicos. Actualmente estamos elaborando nuestro plan estratégico, pero hemos recibido planes estratégicos de Sudáfrica, de Kenia, de Ghana, así que compartimos esos documentos. [...] También compartimos algunas de esas documentaciones [reglamentarias], que nos ayudan, sobre todo a nosotros, que no podemos contratar inmediatamente a consultores para que nos hagan este trabajo [de redacción]. [...] La colaboración es muy importante.

[91] Pisa and Nwankwo, "*Are Current Models of Data Protection Fit for Purpose*?"

> Ya se está llevando a cabo en el seno de los comisarios de protección de datos. Y creo que sólo podemos mejorarla, pero es algo que todos reconocemos que es necesario para nosotros.

Además de compartir las mejores prácticas y los documentos regulatorios, algunos de los entrevistados que están desarrollando su capacidad en materia de APD también informaron de que estaban comparando sus progresos con los de otros organismos de la región.

La asociación con APD regionales también puede fortalecer la capacidad colectiva para influir en las grandes empresas tecnológicas extranjeras. Como declaró Thelma Quaye de SmartAfrica, «Si los países africanos presentan un frente unido en la política de datos, como los Estados miembros de la UE, tendrían un mayor poder para influir y cambiar el comportamiento de estas empresas».[92] Por ejemplo, la actualización de la política de privacidad de Meta de marzo de 2021 para WhatsApp, que anunció que el servicio de mensajería compartiría los datos de los usuarios en los servicios de la empresa matriz, incluido Facebook, violó la POPIA (Ley de Protección de Datos Personales), la ley de protección de datos de Sudáfrica.[93] La APD del país elevó el tema a la Asamblea Global de Privacidad, de la que es miembro, para presionar a Meta a cumplir con su ley.[94] Como dijo un entrevistado,

> Somos tan pequeños que pensamos que, como Asamblea Mundial de la Privacidad, si nos ocupamos de este asunto, seguro que llegaremos a alguna parte. Todavía estamos conversando con la asamblea sobre el enfoque que deberíamos tomar, pero creo que esos son algunos de los temas que, si estamos tratando con un gran jugador como WhatsApp o Facebook, será importante para nosotros como Autoridades de Protección de Datos en el mundo, unirnos en un intento de obligar a grandes jugadores como esos a cumplir.

Además de aumentar la capacidad de aplicación de la ley contra las grandes empresas de tecnología, la colaboración regional también es a menudo un requisito previo para investigaciones efectivas, particularmente dada la naturaleza cada vez más internacional de los flujos de datos. Como declaró un exregulador latinoamericano:

> Hoy en día, cuando se quiere investigar alguna [...] infracción de la ley en términos de protección de datos, es muy posible que necesite investigar algo que [también] tiene lugar en otro país. Por lo tanto, también se debe contar con la cooperación de las otras agencias que están en otro país. [...] Si ve lo que está

[92] Ibíd., 2.
[93] Reuters, "*Regulador sudafricano busca asesoramiento legal sobre la nueva política de privacidad de WhatsApp*."
[94] Duncan McLeod, "*South Africa Threatens Litigation over New WhatsApp Privacy Policy*", TechCentral, 14 de mayo de 2021, https://techcentral.co.za/south-africa-threatens-litigation-over-new-whatsapp-privacy-policy/170079/.

pasando en Europa, con el RGPD me refiero a que las diferentes APD colaboran. El problema en América Latina es que queremos colaborar, pero la colaboración no es algo que esté ocurriendo, que se esté llevando a cabo ahora mismo. Por lo tanto, es muy difícil investigar las violaciones de la protección de datos personales cuando no se tiene la posibilidad de investigar o conseguir alguna prueba que esté en el extranjero.

Estas observaciones también se extienden a África, donde muchas economías regionales están fragmentadas y tienen mercados pequeños. En consecuencia, las empresas tecnológicas regionales tienen incentivos para ampliar sus operaciones más allá de las fronteras nacionales.[95] Sin embargo, las regulaciones de protección de datos en toda la región son inconsistentes, estipulan diferentes reglas para el acceso a la información del usuario, la eliminación y las notificaciones de violación de datos, y requieren diferentes protecciones para los datos confidenciales.[96]

El panorama regulatorio fragmentario puede aumentar los costos de cumplimiento para las empresas que operan transnacionalmente, lo que crea incentivos para que los reguladores africanos armonicen sus leyes de protección de datos.[97] La colaboración entre las APD es fundamental para este esfuerzo. Durante la última década, los países africanos han articulado varios marcos regionales de protección de datos, incluido el prominente Convenio de la Unión Africana sobre Seguridad Cibernética y Protección de Datos Personales de 2014, conocido como el Convenio de Malabo.[98] Otros incentivos para la armonización provienen del Tratado de Libre Comercio Continental Africano (AfCFTA), que promueve la integración del mercado regional, la interoperabilidad y la salvaguardia de los flujos de datos regionales.[99] Como señaló un regulador africano, el establecimiento de un marco regional común puede aumentar el cumplimiento y ayudar a llevar a cabo acciones de aplicación contra las grandes empresas tecnológicas: «Si nos pusiéramos de acuerdo: 'Estos son los principios que se deben cumplir', y nos aseguráramos de que [las grandes empresas tecnológicas] lo hacen en toda la región africana, esa colaboración también nos permitiría llegar a esa ventaja que [nuestra APD] no podría asumir». Sin embargo, ni la Convención de Malabo ni los otros marcos han sido ratificados, y la protección de datos africanos sigue siendo predominantemente el dominio de las leyes y regulaciones nacionales.[100]

Esos esfuerzos de armonización se ven socavados por la falta de una infraestructura jurídica global, como la de la UE, que podría apoyar la aplicación y el cumplimiento de la

[95] Ademuyiwa y Adeniran, "*Assessing Digitalization and Data Governance Issues in Africa*."
[96] Davis, "*Data Protection in Africa: A Look at OGP Member Progress*."
[97] Pisa y Nwankwo, "*Are Current Models of Data Protection Fit for Purpose?*"; Davis, "*Data Protection in Africa*: *A Look at OGP Member Progress*."
[98] Adeyoju, "*Data Privacy Harmonisation in Africa"; Bryant, "Africa in the Information Age*."
[99] Adeyoju, "*Data Privacy Harmonisation in Africa*."
[100] Ibíd.; Bryant "*Africa in the Information Age*."

integración regional.[101] Además, la colaboración también se ve frustrada por la experiencia técnica y regulatoria inconsistente en toda la región y, a veces, por objetivos políticos y regulatorios contradictorios. Algunos reguladores pueden preferir marcos de protección de datos más sólidos o diferentes a los de sus colaboradores regionales, lo que contribuye a crear fricciones o desacuerdos.[102] A pesar del deseo de colaborar y compartir experiencias, los entrevistados también mencionaron las barreras culturales y lingüísticas como obstáculos ocasionales para establecer asociaciones eficaces, tanto entre las regiones como dentro de ellas. Por ejemplo, un regulador africano señaló:

> Creo que los anglófonos se comportan de forma diferente a los francófonos. A veces eso puede dificultar esa colaboración porque, creo, a veces no nos entendemos del todo. [...] Algunos son muy burocráticos. Los anglófonos prefieren establecer los principios y permitir que la gente trabaje. Los franceses, establecen los principios, luego quieren pasar por un período de entrenamiento para que puedan tomar una decisión [sobre los principios]. Así que hay algunas diferencias.

Además, a nivel práctico, el trabajo con las APD regionales puede llevar mucho tiempo y requerir una coordinación significativa. Esta colaboración requiere una estructura: hay que fijar reuniones y asistir a ellas, y definir y seguir sus objetivos. Como señaló un exregulador latinoamericano, las redes de colaboración son tan fuertes como los nodos que las constituyen, y requieren una confianza significativa para operar de manera efectiva. Construir esta confianza puede ser un reto, dado que los reguladores que dirigen las APD cambian. Los organismos regionales de coordinación, como la Red Iberoamericana de Protección de Datos (RIPD) en América Latina, pueden resolver algunos de estos problemas. Sin embargo, como dijo un defensor de la sociedad civil africana, «reunirse es una cosa y hacer cambios de verdad es otra». Aunque los reguladores de las APD se reúnen e intercambian las mejores prácticas, su aplicación depende de los recursos, la fuerza de voluntad y otros factores que pueden socavar una aplicación regional más cohesionada.

Por último, la participación en foros internacionales para la colaboración regulatoria inevitablemente puede reflejar desigualdades globales históricas. Por ejemplo, un regulador africano reflexionó sobre las experiencias recientes con las redes reguladoras mundiales sobre privacidad y acceso a la información:

> Cuando miro la Red Global de Privacidad, creo que las voces de los países africanos están un poco silenciadas, no a propósito. Pero me refiero a todas partes. [...] Hay una conferencia que se va a celebrar en México: la Conferencia General Anual de la ICIC [Conferencia Internacional de Comisarios de Información], que trata del acceso [a la información pública]. He mirado el

[101] Adeyoju, "*Data Privacy Harmonisation in Africa*."
[102] Ibíd.

> programa. No hay ningún africano en ese programa. Y entonces, tengo que decir, pero ¿cómo es que no hay ningún africano en el programa? [...] Así que todo el tiempo hay que luchar por el espacio. De lo contrario, si no luchas, nos olvidan.

Por lo tanto, mientras que las APD del Sur Global pueden beneficiarse significativamente de la participación en redes regionales, pueden en cambio experimentar la marginación en los foros internacionales.

Colaboración con las agencias reguladoras nacionales

Las APD también colaboran con los reguladores de las agencias reguladoras locales, como las que supervisan la política de competencia, la protección del consumidor y la regulación financiera. A medida que la digitalización se expande, la regulación de datos se cruza con un número creciente de dominios de políticas, y la colaboración entre varios reguladores es cada vez más necesaria. Como lo describió un regulador africano,

> Colaboramos con instituciones que podrían tener un mandato superpuesto, por así decirlo, o áreas que son similares como la Comisión de la Competencia, por ejemplo, como la Comisión Nacional del Consumidor. Firmamos memorandos de entendimiento. Pero no solo eso. También colaboramos con la Comisión Electoral que gestiona las elecciones. [...] Tienen que procesar datos en sus listas de votantes, ya sabe. Por lo tanto, tenemos colaboración con organizaciones similares que son de naturaleza regulatoria.

Sin embargo, tal colaboración es desigual. Por ejemplo, los representantes de la sociedad civil latinoamericana argumentaron que la comunicación interregulatoria suele producirse de manera informal, en lugar de un nivel administrativo formal que dé lugar a acciones vinculantes y esté abierto al escrutinio público. Además, las nuevas APD pueden tener menos experiencia y ser más lentas que otras agencias, lo que interrumpe la posible armonización. Por ejemplo, en marzo de 2021, la APD brasileña investigó la actualización de la política de privacidad prevista por Meta, que pretendía integrar los flujos de datos entre el servicio de mensajería WhatsApp, utilizado por más de la mitad de la población[103] del país, y otros servicios de Meta. Según los entrevistados, la APD tardó en analizar el caso, lo que a su vez atrasó a otras agencias.

A veces, la falta de independencia de las APD también puede crear fricciones de colaboración; pueden estar menos dispuestas a abordar investigaciones en el sector público que otras agencias más independientes, con más libertad para hacerlo. Por otro lado, el potencial de colaboración puede verse limitado cuando la APD debe sancionar a

[103] Joen Coronel, "*Whatsapp Upcoming Privacy Update Sparks Uproar in Brazil; Data Protection and Privacy Rights Among Concerns,*" Tech Times, 16 de abril de 2021, https://www.techtimes.com/articles/259192/20210416/whatsapp-upcoming-privacy-update-sparks-uproar-brazil-data-protection-rights.htm.

otra agencia reguladora por prácticas de datos no conformes. Como relató un regulador africano:

> Durante el manejo de COVID, el Departamento Nacional de Salud se convirtió en custodio de una gran cantidad de datos de personas que dieron positivo [para realizar el rastreo de contactos]. Las regulaciones que adoptamos bajo la Ley Nacional del Estado de Desastre dicen: seis semanas después del final del estado nacional de desastre, el Departamento Nacional de Salud debe eliminar esa información o desidentificarla si desean usarla para tales fines. Y tan pronto como el estado nacional de desastre llegó a su fin [...] regresaron y dijeron: «Bueno, danos un mes». Todavía no lo han hecho. Por lo tanto, significa que nos obligarán a usar nuestros poderes para obligarlos a hacerlo.

Por consiguiente, si bien la colaboración con otras instituciones reguladoras nacionales es cada vez más esencial, esos organismos pueden ser objeto de medidas coercitivas.

Colaboración con las organizaciones de la sociedad civil

Las organizaciones de la sociedad civil son socios decisivos de las APD. Como señaló un actor de la sociedad civil africana, «el papel más importante de las OSC [organizaciones de la sociedad civil] sería supervisar y garantizar la rendición de cuentas en cualquier forma que pudiera ser necesaria en la etapa en que se encuentra el país». Otro se refirió a ambas partes como «aliados naturales». Por ejemplo, los entrevistados de las APD africanas mencionaron como especialmente útiles las campañas de la sociedad civil para sensibilizar al público sobre la protección de datos y las capacitaciones para diversos actores del sector privado, incluidos los sectores de la salud, los seguros y los medios de comunicación. Las capacitaciones ayudaron especialmente a aumentar el cumplimiento normativo. Como señaló un entrevistado, las organizaciones de la sociedad civil a veces tienen un mayor alcance público que las APD, lo que les da una ventaja en la elaboración de campañas de sensibilización eficaces. En términos más generales, las organizaciones de la sociedad civil en el Sur Global desempeñan un papel vital como vigilantes: un regulador africano señaló que un informe de la sociedad civil en el país dio lugar a la primera investigación de la DPA. Asimismo, como relató un representante de la sociedad civil latinoamericana, a menudo «después de dirigirnos a los medios de comunicación y presentar una denuncia, una queja pública, las autoridades empiezan a investigar» a la parte infractora.

Además, las organizaciones de la sociedad civil colaboran en las investigaciones y la aplicación de la ley. Un entrevistado de una destacada organización de la sociedad civil latinoamericana argumentó que el principal objetivo de la organización es reforzar y apoyar la APD mediante la sensibilización sobre la protección de datos y la asistencia en los litigios. Dicha asistencia puede implicar hacer presentaciones *amici curiae* a los tribunales y proporcionar a las APD argumentos legales y técnicos para ganar casos de protección de datos. Por ejemplo, las organizaciones de la sociedad civil desempeñaron

un papel clave en la asistencia a la APD brasileña para hacer frente a la actualización de la política de privacidad de 2021 de Meta para WhatsApp. No solo crearon un sentimiento de urgencia en torno al caso, llamando la atención del público sobre el problemático cambio de privacidad de la empresa extranjera, sino que también asesoraron a los reguladores en su investigación.

A pesar de la relación aparentemente natural entre la sociedad civil y las APD, varios factores pueden frustrar las colaboraciones efectivas. Las organizaciones de la sociedad civil dependen del apoyo de los donantes y, al igual que las APD, pueden enfrentarse a limitaciones de recursos, lo que puede socavar su capacidad para sensibilizar al público, supervisar el espacio de protección de datos y ayudar en las investigaciones y los procedimientos de aplicación. Además, la capacidad de las organizaciones de la sociedad civil para participar en estas actividades y desarrollar relaciones con los reguladores depende de la salud del espacio cívico. Como señaló un defensor de la sociedad civil africana:

> Si el espacio cívico se cierra [...] puede presentar retos muy difíciles para el trabajo como la incidencia o el desarrollo de capacidades y todo eso. Y si además hay una falta de confianza o la relación entre la sociedad civil y el ejecutivo es muy limitada, a veces cuando se intenta introducir en la sala al ejecutivo, se encuentra esa animosidad. Y también nos enfrentamos al reto de la falta de interés general del ejecutivo.

Los representantes de la sociedad civil de varios países africanos y latinoamericanos informaron de los problemas relacionados con el acceso a los reguladores y a los procedimientos regulatorios. Otro reto, como subrayó un defensor, es «un déficit de competencias dentro de la propia sociedad civil, que hace que los conocimientos [técnicos] se concentren en muy pocas personas», lo que dificulta la contratación de expertos locales. Otros señalaron que los objetivos entre la sociedad civil y los reguladores podían diferir. Por ejemplo, un defensor de África argumentó que las organizaciones de la sociedad civil se acercan a la protección de datos «desde una perspectiva de derechos humanos [mientras] los gobiernos nunca lo hacen realmente». Por el contrario, un regulador observó que las organizaciones de la sociedad civil a veces pueden tener un enfoque único (por ejemplo, defender exclusivamente protecciones de privacidad más fuertes), mientras que los reguladores a menudo deben equilibrar múltiples objetivos, como los derechos de privacidad y el acceso a la información. Además, un regulador africano dijo que la sociedad civil puede carecer de un enfoque «equilibrado» para la defensa de la protección de datos que reconozca que

> muchas de nuestras empresas no pueden innovar si no utilizan datos. Sabemos que los datos son útiles para tomar decisiones con conocimiento de causa, para mejorar la prestación de servicios y cosas por el estilo. Pero la sociedad civil interpreta los datos de una manera muy extrema: 'Son mis datos, no pueden

> utilizarlos'. [...] En muchos casos, ni siquiera apreciará lo que el gobierno ha hecho [como aprobar leyes]. [...] [Esto] crea mucha fricción con la autoridad, que finalmente afecta la manera en que hacemos parte de nuestro trabajo.

Lograr el equilibrio entre salvaguardar los derechos sobre los datos y al mismo tiempo no sofocar las economías digitales emergentes puede causar fricciones entre la sociedad civil y las APD.

Mejores prácticas y recomendaciones para encarar los retos que enfrentan las APD

Los retos identificados con anterioridad a menudo se interrelacionan y se superponen. Por ejemplo, el desconocimiento del público y el hecho de que los políticos dejen de lado las cuestiones relacionadas con la protección de datos no sólo frustran los esfuerzos para establecer las APD, sino también para garantizar su financiación, contratar expertos, garantizar el cumplimiento y hacer cumplir eficazmente las leyes de privacidad. Del mismo modo, la aplicación efectiva de la ley requiere una financiación suficiente, una independencia sólida, una importante sensibilización del sector público y privado sobre los derechos de privacidad y las leyes de protección de datos, y un amplio grado de cumplimiento. En consecuencia, los problemas de las APD suelen estar relacionados entre sí y, por tanto, requieren soluciones múltiples. Al mismo tiempo, las soluciones individuales pueden abordar más de un problema. De las experiencias de las APD y los actores de la sociedad civil que trabajan en la protección de datos en África y América Latina han surgido varias buenas prácticas y recomendaciones que se analizan a continuación.

1. Abogar por la independencia de la APD desde el principio refuerza la independencia en el futuro

Dado que la independencia es esencial para una APD eficaz, los reguladores que deseen establecer APD deben hacer de ella una prioridad. Como destacó un participante en la mesa redonda: «si no se afirma la independencia al principio, es realmente muy difícil recuperarla». Varios países ofrecen posibles enfoques estructurales para maximizar la independencia de la APD. Por ejemplo, Mauricio y Sudáfrica gozan de autonomía jurídica, económica y administrativa, y sólo dependen del Parlamento, mientras que la APD de Argelia se rige por un consejo con representantes de todos los poderes del Estado, lo que diluye su influencia individual.[104] Los entrevistados destacaron la importancia de separar los presupuestos de la APD del ejecutivo como otro factor clave. En el caso de las APD existentes que se enfrentan a amenazas a la independencia, la sociedad civil puede desempeñar un papel importante realizando y divulgando

[104] Ademuyiwa y Adeniran, "*Assessing Digitalization and Data Governance Issues in Africa*."

investigaciones independientes e informes públicos, en particular a nivel de las comunidades locales, para fomentar la demanda y la cultura de la independencia.[105]

2. Garantizar el equilibrio entre los valores y las necesidades locales y la protección de datos de referencia desde el principio es esencial para la legitimidad y la eficacia de la APD

Si bien los marcos europeos de protección de datos sirven como un estándar de oro internacional, no se traducen automáticamente en otras regiones, especialmente en ausencia de una infraestructura regulatoria y legal equivalente. La armonización de la reglamentación puede aportar importantes beneficios, incluso con respecto a las transferencias transfronterizas de datos que facilitan la participación en las economías mundiales de datos. Sin embargo, el diseño y la aplicación de los marcos locales de protección de datos exige tener en cuenta las culturas y capacidades jurídicas y regulatorias locales, a menudo únicas, así como las realidades económicas. Concretamente, el diseño puede implicar una serie de consultas con diversos representantes públicos y del sector privado. Dicha participación pública debe complementarse con investigaciones que examinen cómo la explotación de datos y los daños asociados se desarrollan e impactan en diferentes contextos y sectores locales. Del mismo modo, la aplicación de los marcos de protección de datos puede implicar el despliegue del cumplimiento y la aplicación en fases de referencia que garanticen un espacio suficiente para la retroalimentación y el cumplimiento de los sectores público y privado. Si no se cuenta con esa participación y retroalimentación del público y se evalúan cuidadosamente las necesidades y preocupaciones locales, la legitimidad pública de una APD puede verse afectada. Además, los problemas de protección de datos pueden no tener eco en las mismas poblaciones que están en mayor riesgo de que sus datos sean mal utilizados, perpetuando estereotipos sobre la privacidad que son dominio de políticos y élites adineradas.

3. La colaboración con la sociedad civil es esencial para las funciones básicas y la legitimidad de la APD

Como destacaron varios participantes en la mesa redonda, a pesar de los objetivos a veces divergentes, la colaboración con la sociedad civil es esencial para cultivar la conciencia local de los derechos y obligaciones en materia de privacidad. Como señaló un regulador, «hemos visto mucha actividad en la sociedad civil. Creo que es una oportunidad porque son capaces de alzar la voz donde nosotros no lo hacemos. … Colaboramos mucho con ellos, sobre todo en la creación de conciencia para denunciar a las organizaciones que no cumplen». Continúan siendo socios cruciales en la educación del público, lo que puede aumentar la legitimidad de las APD, pero también

[105] Internet Society, "*Personal Data Protection Guidelines for Africa*."

en la sensibilización del sector privado. Particularmente, nombrar y avergonzar a los infractores puede ayudar con la aplicación y mejorar el cumplimiento. Por ejemplo, en América Latina, las ONG han colmado una brecha clave en la aplicación de la ley al abogar por la transparencia en las solicitudes de datos gubernamentales de los proveedores de servicios de Internet; una tarea que está fuera del mandato de muchas APD regionales debido a las exenciones legales para las entidades públicas.[106]

4. La colaboración entre las APD puede aunar recursos, crear conciencia y fortalecer la aplicación

A pesar de ciertos desafíos asociados con la colaboración entre las APD, el consenso abrumador entre los reguladores de datos es que la práctica es inmensamente beneficiosa para despertar la conciencia, fortalecer la aplicación y compartir las mejores prácticas. Como dijo un participante en la mesa redonda, «la cooperación internacional [y] el desarrollo de la cooperación entre los miembros de la red [pueden] mejorar la visibilidad en la escena mundial, crear una red de intercambio con los órganos de África, desarrollar herramientas y el desarrollo de capacidades de los miembros». Otro regulador visitó las APD en Europa y América del Norte para aprender sobre las mejores prácticas como uno de los pasos preliminares para lanzar una comisión africana. También hay oportunidad para la colaboración entre las regiones del Sur Global, pero si bien al menos un marco de protección de datos africano se inspiró en uno latinoamericano, los entrevistados no estaban al tanto de ninguna colaboración explícita.

Tal colaboración y consulta no tiene por qué abrumar los objetivos, valores o necesidades locales, especialmente dado que hay muchas diferencias culturales, económicas y de otro tipo importantes tanto dentro de las regiones como incluso con los países individuales.[107] Más bien, dado que las APD en África y América Latina a menudo enfrentan problemas similares (por ejemplo, limitaciones de financiación, conciencia limitada), la colaboración puede priorizar el abordaje de problemas comunes. Además, la aplicación coordinada puede aumentar la probabilidad de sancionar con éxito el incumplimiento de las grandes tecnologías.[108] Por último, aunque la armonización sigue siendo difícil de alcanzar, los esfuerzos por armonizar los marcos pueden proporcionar una previsibilidad crucial a las empresas que operan a través de las fronteras y, en consecuencia, aumentar el cumplimiento general.

[106] Rodriguez y Alimonti, "*A Look-Back and Ahead on Data Protection in Latin America and Spain*."
[107] por ejemplo, Sutherland, "*The Governance of Data Protection in South Africa*."
[108] Davis, "*Data Protection in Africa: A Look at OGP Member Progress*."

5. La orientación estratégica y el marco de la mensajería, así como la creación de relaciones entre las APD y los medios de comunicación, pueden contribuir a despertar la conciencia

Ciertos esfuerzos de sensibilización son especialmente eficaces. Un enfoque concreto para comunicar al público lo que está en juego en las violaciones de la privacidad es vincular las preocupaciones de protección de datos con los daños concretos de la vida real.[109] Dado que el deseo de participar en las economías globales de datos sirve de fuerte incentivo en el desarrollo de leyes de protección de datos y en el refuerzo[110] de su aplicación, subrayar los beneficios económicos de una fuerte regulación y cumplimiento de los datos puede resonar tanto en el sector privado como en los responsables políticos. Este marco puede aumentar el apoyo de los responsables políticos a las APD y, potencialmente, ayudar al retraso en el cumplimiento al vincular las buenas prácticas de datos del sector privado con el éxito económico. En esta línea, un regulador africano enfatizó la utilidad de las herramientas digitales para llegar a la clase trabajadora conocedora de la tecnología y despertar la conciencia sobre los derechos y responsabilidades de protección de datos: «Tenemos *webinars* mensuales donde hablamos de temas de actualidad, y nuestra asistencia ha sido buena [...] Y estos nos han costado muy poco. [...] Sin poner espacio publicitario en absoluto hemos sido capaces de llegar muy lejos». Otra oportunidad para aumentar la conciencia, como argumentó el anterior regulador, es desarrollar relaciones más sólidas entre las APD y los medios de comunicación. Estas relaciones no solo pueden aumentar la conciencia pública sobre los problemas de protección de datos, mejorando potencialmente el cumplimiento y la aplicación, sino que también aumentan la transparencia en torno a los procedimientos de APD.

6. La colaboración con otras agencias reguladoras, la adopción de un enfoque basado en el riesgo y el fortalecimiento del sistema judicial pueden reforzar la aplicación

Para abordar los retos de la aplicación, que a menudo se ven exacerbados por la financiación y la capacidad limitadas, los expertos abogan por soluciones creativas. Por ejemplo, Suyash Rai, de Carnegie India, sostiene que, dado que «la capacidad de una APD será limitada al principio de su mandato, la institución debería utilizar un enfoque basado en el riesgo para dirigir los recursos a las áreas en las que los riesgos son mayores para evitar la sobrecarga.[111] Además, el uso de *RegTech* (tecnología regulatoria) para automatizar la tramitación de las reclamaciones puede ayudar a resolver los problemas de capacidad. Del mismo modo, dar prioridad a los recursos existentes para

[109] Ibíd.
[110] Bryant, "*Africa in the Information Age*."
[111] Pisa y Nwankwo, "*Are Current Models of Data Protection Fit for Purpose?*", 4.

crear un registro público de infractores como sanción de reputación también puede aumentar el cumplimiento y reducir las cargas de aplicación.[112] Un entrevistado también destacó que la colaboración con otros organismos reguladores de un país puede mejorar la aplicación y el cumplimiento. El entrevistado, un regulador en África señaló la mejora de los índices de cumplimiento en los sectores financiero, de seguros y de telecomunicaciones, argumentando que «el trabajo con los reguladores ha sido realmente útil y es algo que queremos continuar y asegurarnos de traer a más personas a bordo». En general, las APD que tienen mandatos intersectoriales están especialmente bien situadas para lograr la participación de múltiples interesados, incluidos la sociedad civil y otros organismos reguladores.[113] Dado que varios entrevistados relataron desafíos relacionados con la inexperiencia judicial en la adjudicación de casos de protección de datos, el fortalecimiento y la creación de capacidad técnica para los tribunales también es un factor clave para una aplicación más efectiva.[114]

7. Financiar programas de educación puede fomentar la experiencia local y la conciencia pública

Como indica el liderazgo de Sudáfrica en materia de protección de datos en África, abogar por la inclusión de las cuestiones relativas a los datos y la privacidad en el currículum universitario puede aumentar los conocimientos locales y la alfabetización digital.[115] Del mismo modo, un exregulador latinoamericano destacó la importancia de cultivar la experiencia local a través de la educación. Tal esfuerzo requeriría no solo ampliar los programas de estudio en las escuelas de derecho y los departamentos de ciencias de la computación, sino también la educación en alfabetización digital en todas las universidades. La financiación de programas académicos relacionados con la protección de datos y los flujos de datos puede crear una cantera de futuros encargados de hacer cumplir la ley, así como fomentar la conciencia pública y el diálogo en torno a las cuestiones de protección de datos.

8. Apoyar las redes nacionales y regionales de la sociedad civil puede fortalecer las investigaciones sobre el cumplimiento de las normas

Los entrevistados de la sociedad civil destacaron que la creación de redes regionales entre las organizaciones de la sociedad civil dentro de los países y entre ellos puede apoyar las investigaciones sobre el cumplimiento de las normas. Estas redes pueden dar lugar a una ayuda mutua, especialmente en torno a los grandes casos judiciales. Uno de los entrevistados los describió como «efectos de red»: con la colaboración de un número considerable de organizaciones, los defensores fueron más eficaces en la obtención de

[112] Pisa and Nwankwo, "*Are Current Models of Data Protection Fit for Purpose*?"
[113] Ademuyiwa y Adeniran, "*Assessing Digitalization and Data Governance Issues in Africa*."
[114] véase también Abdulrauf y Fombad, "*Personal Data Protection in Nigeria*."
[115] Makulilo, "*Privacidad y protección de datos en África*."

documentos normativos, la elaboración de documentos jurídicos especializados y otras funciones de apoyo. Además, tales redes de colaboración sirvieron como una fuente crucial de apoyo social y motivación para los litigantes civiles involucrados en procedimientos desafiantes y de recursos y tiempo intensivo, como el caso de WhatsApp en Brasil.

9. Fomentar espacios cívicos abiertos y construir redes locales de actores políticos puede proteger y reforzar la independencia y responsabilidad de la APD

Aunque las APD aplican y hacen cumplir los marcos de protección de datos, la protección de datos es en última instancia un esfuerzo de colaboración que requiere redes sólidas y espacios cívicos saludables. La sociedad civil puede ayudar en el fomento de oportunidades y espacios cívicos para construir tales redes donde los actores políticos puedan participar en un debate abierto sobre temas de protección de datos. Un representante de la sociedad civil latinoamericana ofreció un ejemplo de esas reuniones que tuvieron lugar en su país:

> [Creo que es importante] organizar seminarios técnicos en los que las personas puedan hablar libremente sobre lo que piensan sobre cuál debería ser el mejor enfoque regulatorio para la protección de datos. [...] En los últimos diez años, tuvimos [tales] seminarios organizados. [...] La gente, se sintió en un espacio seguro, [...] personas del gobierno, fiscales federales, abogados [...] sociedad civil, activistas, etc. [...] Era un espacio para las conversaciones, y para profundizar en algunas cuestiones de política, e incluso para estar en desacuerdo al final. Pero creo que esto era muy importante para generar confianza. [...] Pienso que esto también fue clave para construir relaciones con los miembros de la APD.

La creación de estructuras que cultiven espacios cívicos sólidos de libre intercambio es esencial para construir redes duraderas de actores políticos que inviertan en el desarrollo de marcos robustos de protección de datos y de supervisión. Incluso cuando el espacio cívico nacional está restringido o cerrado, tales reuniones pueden servir como los pilares de las redes de responsabilidad mutua que proporcionan controles cruciales sobre las amenazas a la independencia regulatoria.

Acerca de los Autores

Pawel (Paul) Popiel es Becario Postdoctoral George Gerbner en Annenberg School for Communication, University of Pennsylvania. Pensilvania. Su investigación examina cómo la política da forma a la gobernanza de los medios digitales y las tecnologías emergentes. Su investigación ha sido publicada en revistas como *Policy & Internet*, *Critical Studies in Media Communication*, *Journal of Digital Media & Policy*, *Journal of Broadcasting & Electronic Media*, y otras, y ha sido presentada en importantes conferencias. Obtuvo su Ph.D. en Annenberg School for Communication, University of Pensilvania. También tiene una licenciatura en Ciencias Políticas de McGill University y una maestría en Estudios de Medios de the University of Texas at Austin.

Laura Schwartz-Henderson es Asesora de Investigación y Defensa en el equipo de Tecnología Global de Internews, donde desarrolla herramientas estratégicas de defensa, programas e investigación sobre políticas tecnológicas, ecosistemas de medios y movimientos sociales. Anteriormente, Laura fue Becaria y Gerente de Políticas para el programa de Democracia Digital del German Marshall Fund y Gerente de Proyectos de Investigación en the Internet Policy Observatory en the University of Pennsylvania's Annenberg School for Communications. Tiene una amplia experiencia en la realización de investigaciones sobre temas de derechos digitales, la gestión de programas y el trabajo con activistas y periodistas en diversos contextos políticos. Laura recibió una maestría en Administración Pública de the University of Pennsylvania. Su investigación se centra en los mecanismos a través de los cuales la tecnología media el compromiso cívico y las arquitecturas institucionales y las culturas de la justicia social y las organizaciones filantrópicas. Es la fundadora de *Creative Digital Rights Advocacy Collab Network* y la productora ejecutiva del podcast *Privacy is Global.*

El Profesor Eduardo Bertoni (PhD, Universidad de Buenos Aires) es actualmente el Representante de la Oficina Regional para América del Sur del Instituto Interamericano de Derechos Humanos. Fue el primer director de la Agencia de Acceso a la Información Pública (AAIP) que es la Autoridad Argentina de Protección de Datos y Acceso a la Información. Fue fundador y primer director del Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) de la Facultad de Derecho de la Universidad de Palermo, Argentina. Fue director ejecutivo de la Fundación para el Debido Proceso Legal (DPLF) hasta mayo de 2006. Anteriormente, fue Relator Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la Organización de los Estados Americanos (2002-2005).