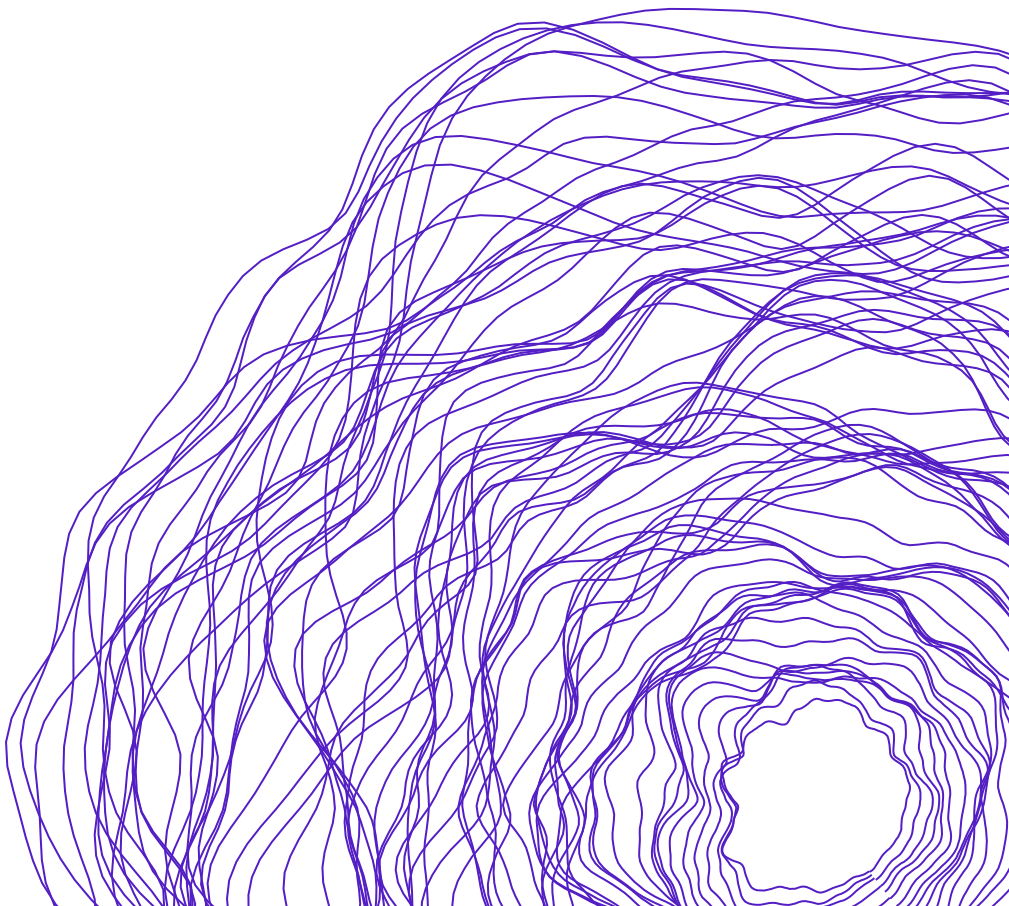
# Entender os desafios que os reguladores de proteção de dados enfrentam: uma luta global rumo à implementação, à independência e ao cumprimento

**Pawel Popiel e Laura Schwartz-Henderson**

**Com prefácio de Eduardo Bertoni**



# Sobre este relatório

Desde 2018, mais de sessenta países em todo o mundo promulgaram ou propuseram novas leis de proteção de dados. Esse número aumenta constantemente a cada ano que passa. Órgãos e agências reguladoras de proteção de dados são os grandes responsáveis pelo cumprimento dessas leis recém-aprovadas em todos os setores da sociedade, com recursos bem insuficientes, pequenos orçamentos e equipe reduzida na maioria dos casos. Muitos países continuam enfrentando a questão da independência, pois esses órgãos geralmente são alojados, financiados ou conectados a ministérios e escritórios executivos, além de serem encarregados de garantir que entidades governamentais e partidos políticos cumpram a lei.

No fim de 2021, o Projeto ADAPT da Internews reuniu um grupo que representa as autoridades reguladoras de proteção de dados (APDs) em 11 países da África e da América Latina para uma mesa redonda, com o objetivo de discutir os desafios que enfrentam na criação, na implementação e no cumprimento das leis de proteção de dados recém-criadas, além de debater as melhores práticas e oportunidades de colaboração transnacionais. Com base nesse diálogo e em entrevistas adicionais com reguladores e os principais informantes da sociedade civil, este relatório procura delinear os principais desafios enfrentados pelas APDs e áreas de apoio e compartilhamento de informações.

Os autores gostariam de agradecer a todos os participantes da mesa redonda e das entrevistas e destacar particularmente os comentários e as contribuições de Eduardo Bertoni, Rafael Zanatta, Luã Cruz, Khadijah El-Usman, Hlengiwe Dube, Benjamin Whitehead e Skyler Sallick

# Índice

## UM BREVE PREFÁCIO BASEADO NA PERSPECTIVA DE UMA EX-APD

Recebi com satisfação o convite para escrever a introdução deste relatório sobre os desafios que os reguladores de proteção de dados enfrentam na África e na América Latina. O documento é baseado em conversas e debates que iniciamos durante uma oficina multilíngue que fui convidado a mediar com 11 reguladores da África e da América Latina. O relatório resultante busca extrair algumas das principais conclusões dessa conversa, com o desenvolvimento dos tópicos discutidos pelos autores durante este evento, incluindo entrevistas de acompanhamento com especialistas de ambas as regiões. Embora o documento a seguir descreva e catalogue com excelência uma série de questões que as APDs devem enfrentar, como independência, financiamento, capacidade técnica e experiência e desafios de cumprimento, pensei que a melhor maneira de iniciar uma discussão sobre esses desafios seria contar uma história mais pessoal sobre o que presenciei como defensor e regulador na América Latina, mais especificamente na Argentina, onde chefiei a Autoridade de Proteção de Dados de 2016 a 2020.

Como mencionei em outro trabalho,[1] nos últimos vinte anos, vários países da América Latina promulgaram as próprias leis de proteção de dados e, em muitos casos, essas leis seguiram normas que foram e ainda estão sendo desenvolvidas na União Europeia. Apesar disso, apenas alguns desses países – a saber, Uruguai, Argentina e México – aderiram à Convenção 108. Além disso, apenas Uruguai e Argentina receberam autorização por "decisões de adequação" que são determinadas regularmente pela Comissão Europeia e aprovadas pela União Europeia.

Os benefícios para quem obtém essas decisões são, entre outros, permitir fluxos de dados gratuitos entre a UE e esses países, de acordo com a Diretiva de Proteção de Dados 95/46/CE (doravante denominada "Diretiva"). Pode não ser coincidência que dois dos três países que ratificaram o tratado (Convenção 108) também tenham sido considerados adequados pela União Europeia. Nesse sentido, pode ser importante mencionar que a Convenção 108 e o GDPR são duas peças do mesmo quebra-cabeça que vem influenciando diversas reformas.

Muitas das novas leis de proteção de dados foram inspiradas tanto pelo GDPR quanto pela Convenção 108. No entanto, a aprovação de regulamentos que atendam a essas normas internacionais não tem sido um trabalho fácil. Em muitos casos, as normas são incompatíveis com a capacidade regulatória, e as reformas necessárias são muito impopulares. Além disso, há muitos desafios a serem enfrentados antes de ter leis que cumpram as normas internacionais. Vários desses desafios geralmente são motivados por questões políticas e econômicas.

[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.

A história da lei argentina de proteção de dados pessoais demonstra dois dos desafios mais importantes enfrentados pelas autoridades de proteção de dados na América Latina e na África. O primeiro deles diz respeito à criação de um órgão que seja independente, tanto na prática quanto no regulamento. O segundo está ligado à "força" que as autoridades de proteção de dados têm para o cumprimento da lei.

Resumidamente, a história é a seguinte: a Argentina reformou sua Constituição em 1994. A reforma introduziu o Artigo 43, que afirma:

*Qualquer pessoa deverá ajuizar esta ação para obter informações a respeito dos dados sobre ela e sua finalidade, registrados em bancos de dados ou registros públicos ou privados, destinados a fornecer informações; e em caso de dados falsos ou discriminação, esta ação poderá ser ajuizada para solicitar a supressão, retificação, confidencialidade ou atualização deles. A natureza sigilosa das fontes de informação jornalística não será prejudicada.*

Pouco antes do início do século XXI, iniciou-se um forte debate na Argentina para aprovar uma lei que regulamentasse concretamente este artigo 43 da Constituição. Assim, em 2000, o Congresso aprovou um projeto de lei de proteção de dados pessoais que incluía duas questões que quero destacar.

A primeira delas refere-se ao fato de que o projeto aprovado pelo Congresso previa a existência de um órgão específico para controlar o cumprimento da lei. Mas, além disso, a lei designava a quem cabia aquele órgão – um Diretor indicado pelo Presidente e aprovado pelo Senado – para garantir independência e autonomia.

A segunda questão diz respeito às multas. Por muitas razões que não estão relacionadas a esta conversa, naquela época, a Argentina tinha uma economia estável, na qual a equivalência entre o dólar norte-americano e o peso argentino era de US$ 1 = AR$ 1. Na ocasião, os políticos estavam convencidos de que a paridade entre o dólar norte-americano e o peso argentino duraria muito tempo. Por isso, muitas das leis que foram aprovadas naquele momento – quando expressavam os valores das multas – não incluíam formas de atualizá-las ao longo do tempo. A multa máxima que foi incluída na conta foi de AR$ 100.000.

Na Argentina, uma vez aprovado no Congresso, um projeto é enviado ao Presidente da Nação para sua aprovação ou direito de veto, que pode ser total ou parcial. Em 2000, o Presidente da Argentina vetou parcialmente a lei e anulou o artigo que define a criação da autoridade de proteção de dados. De acordo com o Decreto nº 995/2000 assinado pelo Presidente, o motivo desse impedimento estava relacionado a questões orçamentárias.

O veto de apenas essa parte do artigo cria um problema: a lei mencionava em geral a existência de um órgão para supervisionar a nova lei de proteção de dados, mas, por causa do veto, ela não forneceu detalhes sobre esse órgão de fiscalização.

Em outras palavras, o resultado foi claro: a Argentina tinha uma lei de proteção de dados pessoais que dizia que havia um órgão responsável por seu cumprimento, mas não descrevia quem era responsável por ele, como essa pessoa poderia ser nomeada ou exonerada ou a localização dessa autarquia. Por isso, no ano seguinte, o Presidente, ao regulamentar a lei, criou o referido órgão, mas como uma Diretoria dentro do Ministério da Justiça e Direitos Humanos. Seu Diretor poderia ser nomeado ou exonerado pelo Ministro da Justiça como qualquer outro empregado.

Por esse motivo, a independência e autonomia da autoridade de proteção de dados foi bastante afetada, despertando dúvidas internacionais sobre a real independência da APD recém-criada. Apesar desse regulamento insatisfatório, a Argentina defendeu perante a União Europeia e o Conselho da Europa que o órgão vinha atuando de maneira independente. Esses argumentos foram bem sucedidos na ocasião e a Argentina foi considerada um país com legislação adequada. Para agravar esta questão muito crítica com a independência estrutural da APD, a inflação no país vem aumentando consideravelmente nos últimos 20 anos. Não existe mais aquela paridade entre o peso argentino e o dólar norte-americano. Portanto, a multa máxima que pode ser imposta hoje pela autoridade de proteção de dados na Argentina é de apenas quinhentos dólares norte-americanos.

Ao longo de muitos anos, eu e muitos outros especialistas e defensores afirmamos que uma mudança no regulamento era cada vez mais necessária e exigida. Isso finalmente aconteceu em 2017. Conseguimos alterar os regulamentos necessários para incluir a APD no âmbito da então recém-criada Agência Nacional de Acesso à Informação, um órgão independente criado por lei com orçamento próprio e com o esclarecimento específico de que o Diretor não poderia ser demitido pelo Presidente sem ter o consentimento do Congresso.

A história da lei argentina e a evolução da APD, uma das primeiras da região, deixa várias lições para todos os países que estão elaborando ou implementando novas leis.

Novas leis de proteção de dados devem ser construídas por meio de consultas e consensos significativos entre as diferentes partes interessadas (sociedade civil, setor privado, mundo acadêmico e alguns órgãos governamentais específicos, como Bancos Centrais, Secretaria da Receita Federal etc.) para que a autoridade de proteção de dados seja independente e autônoma e que isso esteja previsto na lei. Ao elaborar leis de proteção de dados, a importância da independência das autoridades de proteção de dados não pode ser subestimada e há necessidade de mecanismos claros para o cumprimento da lei. As leis de proteção de dados devem ser sólidas, mas também flexíveis para futuras mudanças tecnológicas, políticas e econômicas. As multas também devem ser dissuasivas, de modo que aqueles tentados a infringir a lei não o façam.

Para ser claro: as lições aprendidas com o caso da Argentina são muito mais do que essas mencionadas acima, mas não posso subestimar a importância da independência da APD, principalmente os seguintes tópicos essenciais:

- A independência da APD é fundamental para o sucesso de qualquer regulamento de proteção de dados.
- A independência deve ser garantida por lei.
- A independência deve ser aceita na prática por diversas partes interessadas.
- A independência também significa dar às APDs recursos suficientes para o cumprimento de seus deveres.
- A independência também significa ter uma equipe com experiência suficiente para conduzir investigações sérias.

Mas o trabalho à frente não para com essas diversas questões. Agora, os avanços na tecnologia são muito rápidos. Além disso, nesta era, possíveis violações dos dados pessoais localizados em um país podem ocorrer fora das fronteiras onde as autoridades de proteção de dados desses países estão localizadas. Portanto, é necessário gerar mecanismos que permitam às APDs realizar investigações transnacionais e até mesmo impor sanções a empresas não localizadas em seus territórios. O relatório a seguir busca agregar as perspectivas de vários reguladores, especialistas e defensores para entender melhor como alguns desses desafios ocorrem em diferentes jurisdições. No final do relatório, também extraímos algumas das melhores práticas sugeridas para APDs individuais, bem como para colaboração entre agências reguladoras e sociedades civis no país e entre nações. Esperamos que este documento possa ser usado como ferramenta por defensores, formuladores de políticas e reguladores em todas as etapas do processo legislativo e regulatório.

A criação de leis e estruturas regulatórias compatíveis com a proteção dos dados dos cidadãos, uma tarefa complexa e em constante evolução, não é algo fácil. Mas vale muito a pena tentar. A proteção de dados pessoais está intimamente relacionada ao direito humano à privacidade. Portanto, quando trabalhamos para evitar violações de um direito humano, todo esforço e criatividade são bem-vindos.

# Introdução

Em decorrência da crescente difusão do acesso à Internet nas regiões do Sul Global e da rápida expansão e integração das economias de dados globais,[2] os fluxos de dados regionais envolvem mais usuários em uma gama crescente de atividades diárias. Embora a participação nessas economias possa proporcionar maior inovação e crescimento econômico, juntamente com outros possíveis benefícios, ela também apresenta danos significativos. Por exemplo, a expansão das infraestruturas de dados aumentou a capacidade de projetos de vigilância do Estado, incluindo o acúmulo de dados pessoais de pessoas físicas.[3] Da mesma forma, o aumento do uso de dados pelos setores público e privado aumenta as preocupações com segurança cibernética e levanta questões importantes sobre a responsabilidade dos controladores e operadores de dados.[4] A coleta de dados contínua e cada vez maior, realizada por uma ampla gama de entidades privadas, que variam de empresas de mídia social a bancos comerciais e agências de crédito, agrava essas preocupações com segurança, ao mesmo tempo em que intensifica os riscos de direcionamento comportamental e imprecisão de dados, o que pode resultar na prestação discriminatória de serviços públicos e privados essenciais.[5]

Os marcos de proteção de dados e as agências reguladoras responsáveis por seus cumprimentos são mecanismos essenciais para controlar esses fluxos de dados. No entanto, apesar do progresso considerável no Sul Global para a implementação desses marcos, os atrasos persistem. Atualmente, 71% dos países do mundo têm alguma legislação de proteção de dados, incluindo 73% na América Latina, em relação à África e à Ásia, com 61% e 57%, respectivamente.[6] Como a legislação do Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia estabeleceu a norma global para o regulamento de proteção de dados, a incapacidade de impor proteções igualmente robustas marginaliza economicamente os países do Sul Global que não as possuem, enquanto aumenta os riscos locais de vigilância, a coleta não consentida e o uso indevido

[2] UNECLAC, "Data, Algorithms and Policies: Redefining the Digital World" (Comissão Econômica das Nações Unidas para a América Latina e o 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: Comissão Econômica das Nações Unidas para a América Latina e o Caribe (CEPAL), 2019), https://repositorio.cepal.org/bitstream/handle/11362/44629/1/S1900395_en.pdf.

[3] Lukman Adebisi Abdulrauf e 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] Ibid.

[5] Ibid.

[6] UNCTAD, "Data Protection and Privacy Legislation Worldwide", Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD), acessado em 30 de abril de 2022, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

de dados.[7] Além disso, em países que aprovaram essa legislação, como na maioria da América Latina, os marcos de proteção de dados existentes variam em escopo, implementação e nível de cumprimento.[8]

A tarefa de garantir a conformidade com as leis de proteção de dados, que geralmente exige a educação do setor público e privado sobre direitos de privacidade e obrigações de dados, cabe às Autoridades de Proteção de Dados (APDs). Esses órgãos reguladores – muitas vezes estabelecidos com a aprovação da legislação de proteção de dados, embora nem sempre – enfrentam uma série de desafios no Sul Global que afetam sua capacidade operacional, capacidade de cumprimento e independência regulatória. Muitos fatores contribuem para esses desafios, incluindo restrições de recursos, alfabetização digital limitada entre o público, tribunais inexperientes e formuladores de políticas céticos.

Para iluminar e avaliar os fatores, este documento analisa os desafios enfrentados pelas APDs na África e na América Latina. A análise do relatório baseia-se em resultados de pesquisas que envolveram duas etapas. A primeira delas consistiu em pesquisa documental reunindo o trabalho de especialistas, incluindo reguladores de dados, defensores da proteção de dados e acadêmicos sobre a implementação e aplicação de marcos de proteção de dados no Sul Global. Para a segunda etapa, como parte de seu projeto ADAPT (*Advocating for Data Accountability, Protection and Transparency* - Defesa do Controle, da Proteção e da Transparência de Dados), a Internews convocou uma mesa redonda de reguladores de proteção de dados da Argentina, Brasil, Burkina Faso, Chile, Maurício, Marrocos, Níger, Peru, África do Sul e Uganda em novembro de 2021. Essa discussão gravada foi traduzida, transcrita e codificada, e seus temas servem de base para os temas e questões discutidos neste relatório. As observações da mesa redonda também foram complementadas com oito entrevistas realizadas com reguladores atuais e antigos da APD, alguns dos quais participaram da mesa redonda, bem como representantes da sociedade civil de ambas as regiões. As respostas dos participantes da mesa redonda e da entrevista são anonimizadas no relatório.

Ambas as etapas da pesquisa envolveram a identificação de desafios concretos enfrentados pelas APDs na implementação e no cumprimento dos marcos de proteção de dados, bem como as melhores práticas para resolvê-los. Embora o relatório destaque os desafios compartilhados enfrentados pelas APDs na África e na América Latina, ele também destaca diferenças significativas nessas regiões e entre elas. No entanto, apesar de avaliar obstáculos pouco estudados à proteção de dados em uma amostra de países africanos e latino-americanos, este documento apresenta limitações geográficas.

[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.

Pesquisas futuras devem incluir perspectivas de outras regiões para ampliar a consideração de desafios únicos e compartilhados por APDs no Sul Global.

Com base na pesquisa documental e nos dados qualitativos da mesa redonda e da entrevista, este relatório avalia os desafios relacionados:

1) À criação de uma APD
2) Ao financiamento e à capacidade das APDs
3) À independência na estrutura e na tomada de decisões
4) À conformidade e conscientização
5) Ao cumprimento
6) À abordagem de questões políticas emergentes
7) À colaboração com outras APDs e com a sociedade civil dentro de cada região e entre elas

Dentre as opções acima, dois fatores proeminentes surgiram como principais obstáculos à supervisão eficaz da proteção de dados nas duas regiões examinadas neste relatório: restrições de recursos e ameaças à independência. As restrições de recursos prejudicam a capacidade das APDs de aumentar a conscientização sobre as leis de proteção de dados, contratar especialistas, conduzir investigações e buscar ações de fiscalização, principalmente contra big techs. As ameaças à independência geralmente agravam as restrições de recursos, principalmente quando a organização controladora de uma APD ou o poder executivo do governo controla o orçamento. Elas também prejudicam o cumprimento efetivo, principalmente do setor público, que cada vez mais se envolve na coleta e no tratamento de dados em muitos países da região.

Além disso, o relatório identifica as melhores práticas e recomendações essenciais para enfrentar esses desafios. Em particular, os entrevistados destacaram a colaboração entre as APDs regionais e entre as APDs e a sociedade civil como estratégias especialmente úteis para aumentar a conscientização dos setores público e privado, reunir recursos, compartilhar as melhores práticas, aumentar a experiência e auxiliar no litígio e no cumprimento. Além disso, essas redes de políticas também podem promover a responsabilidade mútua, potencialmente compensando ou reduzindo as ameaças à independência da APD. Os entrevistados também observaram que uma prioridade relacionada envolve o reforço da educação regional para facilitar o cultivo de conhecimentos locais e conscientização em nível comunitário sobre direitos e leis de proteção de dados. Essa experiência e familiaridade são essenciais para um cumprimento eficaz, alta conformidade com os regulamentos de proteção de dados e para tornar as questões de proteção de dados como prioridades políticas e sociais.

# Desafios enfrentados pelas APDS

Os marcos de proteção de dados proliferaram na África e na América Latina na última década. A adoção desses marcos e a criação de APDs ocorreram em parte como resposta às pressões criadas pela aprovação do GDPR e, principalmente na América Latina, pela Convenção 108 do tratado internacional de proteção de dados do Conselho da Europa (CoE), ratificado por países como Argentina, Cabo Verde e Uruguai.[9] Esses processos legais e regulatórios também foram acelerados pelo aumento da difusão tecnológica nas duas regiões. No entanto, o progresso tem sido desigual e os marcos de proteção de dados variam em escopo e robustez. Por exemplo, na América Latina, o Brasil liderou ao aprovar a Lei Geral de Proteção de Dados Pessoais (LGPD), inspirada no GDPR, enquanto a Argentina não atualizou sua legislação pré-GDPR.[10] Na África, países como Ruanda e Zâmbia aprovaram sua primeira legislação de proteção de dados em 2021, enquanto Cabo Verde e Burkina Faso atualizaram suas leis existentes, sendo que o primeiro excedeu alguns requisitos do GDPR.[11] Da mesma forma, países com marcos existentes, como Quênia e África do Sul, emitiram novos regulamentos.[12] No entanto, muitas leis na região não garantem direitos básicos como privacidade e novos, como portabilidade de dados, ou fornecem medidas de responsabilidade importantes, como requisitos para documentar o tratamento de dados.[13]

Embora a elaboração de uma legislação robusta e a criação de uma APD eficaz sejam a base de uma sólida proteção de dados, os países da África e da América Latina enfrentam ou enfrentaram uma série de desafios nesses estágios iniciais, desde a proteção do apoio político até a garantia da independência regulatória. Uma vez estabelecidas, as APDs devem atravessar barreiras para garantir a conformidade

[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; Conselho da Europa, "Chart of Signatures and Ratifications of Treaty 108," Conselho da Europa, 2022, https://www.coe.int/en/web/conventions/full-list; Conselho da Europa, "Chart of Signatures and Ratifications of Treaty 223", Conselho da Europa, 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] A introdução de Eduardo Bertoni a este relatório discute o marco argentino com mais detalhes. Ver também, Gilberto Martins de Almeida, "International: A Brief Perspective on Data Protection in Latin America," DataGuidance, janeiro de 2022, https://www.dataguidance.com/opinion/international-brief-perspective-data-protection; Katitza Rodriguez e Veridiana Alimonti, "A Look-Back and Ahead on Data Protection in Latin America and Spain," Electronic Frontier Foundation, 21 de setembro 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, 1º de fevereiro de 2022, https://www.engage.hoganlovells.com/knowledgeservices/news/recent-developments-in-african-data-protection-laws-outlook-for-2022_1_1.

[12] Ibid.

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

regulatória, incluindo restrições significativas de recursos que dificultam o cumprimento, mecanismos de sanção limitados e inexperiência judicial; falta de conscientização pública sobre leis de privacidade e direitos e obrigações de proteção de dados; e intervenções estatais ocasionais que minam sua independência e legitimidade regulatória. Tais obstáculos servem de contraponto à expansão promissora dos marcos de proteção de dados na África e na América Latina. Essas barreiras devem ser abordadas para maximizar os benefícios da participação regional nas economias de dados globais em termos que reflitam os valores e as necessidades locais, minimizando os danos associados.

## Criação de uma Autoridade de Proteção de Dados

Os desafios centrais na criação de APDs estão relacionados à formação de apoio político inicial, elaboração e aprovação de marcos sólidos de proteção de dados e estruturação da agência. Primeiro, os formuladores de políticas devem elaborar e aprovar legislação que estabeleça um marco de proteção de dados e defina a estrutura, o mandato e o escopo da APD que implementará e aplicará esse marco. O primeiro passo nesse processo requer convencer o governo, o público e o setor privado de que a proteção robusta de dados deve ser uma prioridade política, muitas vezes em meio a outros objetivos prementes. Cultivar esse apoio representa um desafio fundamental, principalmente na África, onde menos leis de proteção de dados foram aprovadas do que em outras regiões e onde persistem lacunas significativas na conscientização pública sobre questões de proteção de dados.

A elaboração de um marco de proteção de dados também requer a contribuição de especialistas locais em regulamentação internacional de proteção de dados e em tecnologias e mercados de uso intensivo de dados para garantir que essa legislação não seja apenas abrangente, mas também sintonizada com contextos, necessidades e valores locais. Essa experiência é especialmente crucial para navegar pela imensa influência que os marcos regulatórios da UE exercem na proteção internacional de dados e para criar APDs que representam interesses políticos, econômicos e sociais locais. No entanto, a escassez desses especialistas, particularmente proeminentes na África, representa outro desafio fundamental para a criação de uma APD. Na ausência dessa expertise, a legislação que define a criação de APDs pode carecer de clareza. Essa ausência de clareza organizacional pode dificultar a construção da capacidade institucional de uma nova APD, na qual os reguladores geralmente devem se envolver enquanto realizam seu trabalho regulatório diário de cumprir o mandato de proteção de dados. Esse trabalho duplo, por sua vez, pode sobrecarregar bastante os recursos já limitados. Além disso, sem essa clareza, as APDs podem enfrentar ameaças à independência ou não ter mandatos suficientemente amplos para equilibrar a proteção de dados com domínios regulatórios relacionados, como acesso a informações, prejudicando o cumprimento efetivo. Esses desafios surgiram como um tema essencial

nas entrevistas, refletindo as preocupações dos reguladores africanos e latino-americanos.

### Implementação de um marco de proteção de dados

Embora muitos países da África e da América Latina ofereçam direitos à privacidade garantidos constitucionalmente,[14] um dos maiores obstáculos à criação de APDs envolve convencer as elites políticas de que a proteção de dados deve ser uma prioridade nacional. Isso representa um desafio significativo, principalmente na África, onde as questões de desenvolvimento e o crescimento econômico historicamente têm prioridade sobre outras preocupações.[15] Ao mesmo tempo, os governos veem as leis de proteção de dados com cautela, especialmente se as atividades que eles gerenciam puderem invadir as atividades de vigilância do estado ou expandir os direitos de acesso a dados públicos.[16] Consequentemente, vários marcos de proteção de dados africanos e latino-americanos têm isenções para categorias geralmente vagas, como segurança nacional, serviços de inteligência e setor público de maneira mais ampla.[17]

O desafio de priorizar a proteção de dados em meio a outros objetivos políticos pode ser agravado pela falta de experiência dos formuladores de políticas com privacidade e regulamentação de dados. As principais barreiras para cultivar essa especialização incluem a migração de trabalhadores qualificados para o exterior ou para o setor privado, bem como a escassez regional de instituições de ensino superior que oferecem treinamento em política tecnológica, evidente principalmente na África.[18] A falta de experiência inibe a elaboração de marcos sólidos de proteção de dados, que muitas vezes criam APDs e definem seu escopo regulatório. Por exemplo, os esforços para elaborar uma legislação na Nigéria, que não tem um marco regulatório para proteção de dados, carecem de envolvimento de especialistas, resultando em casos de "cortar e

[14] Ademola Adeyoju, "International: Data Privacy Harmonisation in Africa - Progress, Challenges, and Predictions," DataGuidance, 9 de dezembro de 2020, https://www.dataguidance.com/opinion/international-data-privacy-harmonisation-africa; Rodriguez e 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 e Fombad, "Personal Data Protection in Nigeria."

[16] Abdulrauf e 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 e Alimonti, "A Look-Back and Ahead on Data Protection in Latin America and Spain"; Abdulrauf e Fombad, "Personal Data Protection in Nigeria"; Mpho Ngoepe, "Balancing and Reconciling the Conflicting Values of Information Access and Personal Data Laws in South Africa," em *Information Knowledge and Technology for Development in Africa*, ed. D. N. Ocholloa, N. D. Evans e J. Britz (Cidade do Cabo: 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."

colar",[19] especialmente a contratação de advogados não especializados que copiaram as leis de privacidade estrangeiras. Este processo produziu projetos de lei fracos ou inconsistentes, nenhum dos quais foi aprovado. Além disso, os formuladores de políticas não emitiram relatórios oficiais e declarações públicas sobre proteção de dados, que são cruciais para obter apoio para essa legislação.[20] Os esforços da África do Sul para aprovar a Lei de Proteção de Informações Pessoais nº 4 de 2013 (POPIA), que atualizou o marco de proteção de dados do país, seguiu padrões semelhantes: políticos mostraram pouco interesse em avançar na legislação, cujo conteúdo "foi parcialmente extraído de outros países, com customização limitada"[21] e cuja passagem foi muito lenta. Esses casos contrastam com as redes experientes e resistentes de especialistas em regulamentação descritas pelos entrevistados em países como Argentina, Brasil, Chile e Colômbia, sugerindo que o conhecimento é distribuído de forma desigual na África e na América Latina e entre esses dois continentes.

Como essas experiências africanas sugerem, na ausência de experiência local, os formuladores de políticas que buscam criar APDs podem acabar emulando modelos de proteção de dados estrangeiros, principalmente europeus. No entanto, outros fatores contribuem para essa transferência de política. As regulamentações internacionais de proteção de dados geralmente são influenciadas pelos marcos do Norte Global, especificamente o GDPR da UE, que é considerado o padrão-ouro, e a Convenção 108, principalmente na América Latina. Além da proeminência reputacional do GDPR, a atração do mercado considerável da UE significa que as empresas de tecnologia provavelmente cumprirão a lei em vez de deixar de fazer negócios na Europa. Como o GDPR é mais rigoroso do que a maioria das leis de privacidade e se aplica a qualquer empresa que trate os dados de cidadãos da UE, existem fortes incentivos não apenas para que empresas de fora da UE o cumpram, mas também para que os marcos nacionais de proteção de dados se harmonizem com ele. Este "Efeito Bruxelas",[22] ou seja, a influência regulatória internacional da Europa, molda inevitavelmente os marcos de proteção de dados no Sul Global, especialmente porque os custos da não conformidade, ou seja, a exclusão dos mercados europeus, afetarão os países em desenvolvimento mais pobres de maneira desproporcional.[23]

Embora os países da África e da América Latina busquem a harmonização com o GDPR – principalmente as decisões de adequação concedidas pela UE a nações compatíveis, que facilitam as transferências de dados transnacionais[24]– possíveis desafios também

[19] Abdulrauf e Fombad, "Personal Data Protection in Nigeria," 124.
[20] Abdulrauf e 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* (Nova York, NY: Oxford University Press, 2020).
[23] Mannion, "Data Imperialism"; Adeyoju, "Data Privacy Harmonisation in Africa."
[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.

surgem aqui. Primeiro, as noções de privacidade diferem nos contextos políticos e sociais, aumentando o risco de incongruências e incompatibilidades na tradução de políticas de conceitos, como direitos de dados. A simples cópia do GDPR para facilitar os fluxos de dados transnacionais poderá subjugar os valores e as necessidades regionais e locais daqueles incorporados no marco da UE, que centraliza os interesses de seus cidadãos.[25] No entanto, as práticas de tecnologia variam. Por exemplo, os usos de smartphones diferem drasticamente no Sul Global,[26] as fronteiras da privacidade social podem ser mais imprecisas do que na Europa, e os principais conceitos jurídicos como "dados pessoais" e "identidade digital" também têm diferentes referentes locais.[27] Enquanto a conceituação ocidental refletida no GDPR admite um direito individualizado à privacidade, os países do Sul Global podem priorizar as dimensões comunitárias e relacionais dos direitos de privacidade.[28] Além disso, eles podem equilibrar os direitos de privacidade com outros direitos de maneira diferente dos países ocidentais, por exemplo, priorizando direitos à água ou à saúde que reflitam os valores e as necessidades locais.[29] A falha em conciliar as metas de proteção de dados com as necessidades locais pode intensificar a conscientização pública limitada e o apoio à proteção de dados que os reguladores observam e condenam. Por exemplo, um regulador africano de proteção de dados declarou: "você ainda ouve pessoas que se perguntam se a privacidade e a proteção de dados são importantes." Esse regulador observou que a conscientização limitada é proeminente sobretudo nas áreas rurais e entre a população de baixa escolaridade, incluindo analfabetos. Outro regulador africano foi mais direto: "Algumas pessoas pensam que a proteção de dados é principalmente para os ricos." No entanto, mais do que apenas compreensão pública limitada, essas atitudes provavelmente também refletem os desafios de conciliar modelos de proteção de dados estrangeiros com contextos e necessidades locais. Em segundo lugar, o GDPR foi criado com base em 30 anos de precedentes legais, que muitos países dessas regiões não têm quando elaboram uma nova legislação de proteção de dados. Da mesma forma, a UE dispõe de imensos recursos para implementar e fazer cumprir o seu marco, o que é impraticável para os países em desenvolvimento que enfrentam restrições orçamentais significativas.[30] Por fim, alguns

[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 e David Hutchful, "Research on Mobile Phone Data in the Global South: Opportunities and Challenges," in *The Oxford Handbook of Networked Communication*, por Seyram Avle, Emmanuel Quartey e David Hutchful, ed. Brooke Foucault Welles e 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."

[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),

especialistas argumentam que impor muito rapidamente um marco de proteção de dados rigoroso como o GDPR pode impedir a inovação local essencial para o crescimento econômico regional e a concorrência internacional.[31]

De maneira mais problemática, as leis de proteção de dados às vezes são financiadas ou elaboradas por agentes externos com consequências preocupantes.[32] Como um agente político africano relatou,

> [p]essoas que não vivem no país redigem as leis e, em seguida, o governo é [pressionado] a aprovar a lei para ter acesso à ajuda ou à ajuda adicional. Geralmente, essas coisas estão ligadas, e torna-se um exercício selecionar a lei que está nos estatutos. Quando você tenta realmente aplicá-la ou tem qualquer tipo de mecanismo de implementação, descobre que ninguém recebeu um orçamento para isso.[33]

Além disso, a imposição externa de leis de proteção de dados e a simples cópia delas podem contribuir para um "efeito de transplante", ou seja, baixa demanda por leis estrangeiras para os residentes de uma nação, inclusive por causa da percepção de ilegitimidade, resultando em má implementação.[34] Assim, os formuladores de políticas que estabelecem marcos locais de proteção de dados enfrentam importantes compensações entre a harmonização básica com padrões internacionais – essenciais à previsibilidade regulatória para empresas que operam de maneira transnacional, por exemplo – e as expectativas e prioridades locais, que podem superar as questões de proteção de dados.

### Estruturação de uma APD

A aprovação de leis de proteção de dados robustas e legítimas estabelece a base para APDs eficazes, mas continua sendo apenas o primeiro passo. De fato, embora essas leis geralmente criem APDs,[35] isso nem sempre é o caso; por exemplo, alguns países africanos não têm APDs, apesar de terem legislação de proteção de dados.[36] Além disso, a legislação nacional nem sempre especifica a estrutura de uma APD ou seu mecanismo

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 e Nwankwo, "Are Current Models of Data Protection Fit for Purpose?"

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

[33] Ibid., 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."

[36] Pam Dixon, "ROUNDTABLE OF AFRICAN DATA PROTECTION AUTHORITIES: Status and Response to Privacy Risks in Identity Systems," em *ID4AFRICA 5TH ANNUAL CONFERENCE* (Joanesburgo, África do Sul: The Round Table of African Data Protection Authorities (RADPA, 2019), 13, https://www.id4africa.com/2019/files/RADPA2019_Report_Blog_En.pdf.

de financiamento, como no caso da Costa do Marfim, de Gana e de Malawi.[37] Consequentemente, as APDs variam em idade, estrutura organizacional e mandato, entre outras dimensões.

A ausência de clareza legislativa sobre esses fatores essenciais – principalmente estrutura e orçamento – pode servir como um obstáculo significativo para a função subsequente da agência. Por exemplo, vários participantes da mesa redonda observaram as consequências da legislação que cria APDs dentro ou sob outro órgão regulador, em oposição a uma agência independente, incluindo competição por recursos, falta de um mandato claro e restrições à independência,[38] conforme explorado em mais detalhes nas seções subsequentes deste relatório. Uma questão estrutural relacionada destacada pelos participantes dizia respeito se a legislação criava APDs com um mandato único ou duplo, que combina a supervisão da proteção de dados com áreas regulatórias relacionadas, como acesso à informação e liberdade de expressão. APDs de mandato único, como argumentou um regulador latino-americano, podem criar desafios na harmonização das leis que regem os fluxos de informação:

> Também estamos enfrentando um desafio muito difícil [...] tentando harmonizar a [...] lei geral de proteção de dados com [...] leis de acesso à informação pública [...] [S]e fosse possível concentrar os poderes de execução em uma única entidade, talvez essa harmonização seria mais fácil.

Por outro lado, uma APD de mandato duplo, como argumentou um regulador africano, "funciona para nós porque o direito à privacidade deve ser sempre equilibrado com a liberdade de expressão e o acesso à informação". APDs com mandatos duplos, como na Argentina e na África do Sul, têm um regulador exclusivo com autoridade sobre proteção de dados, transparência e acesso a informações. Em alguns casos, um regulador de transparência é responsável pela proteção de dados ou vice-versa, e a ordem de expansão do mandato influencia como a APD concilia os objetivos conflitantes, na maioria dos casos, entre proteção de dados e transparência.[39] Como um especialista em políticas descreveu a elaboração da legislação de proteção de dados na África, "você começa com sigilo – esse é exatamente o ponto de partida errado [já que] muitos países, que agora têm essas belas leis modelo sobre privacidade e proteção de dados, têm leis chocantes sobre liberdade de mídia, liberdade de expressão, acesso à internet".[40] Como a proteção de dados pode invadir os fluxos de informações, é essencial encontrar o equilíbrio certo que reflita os contextos locais para marcos eficazes.

[37] Davis, "Data Protection in Africa: A Look at OGP Member Progress."
[38] ver também Pisa e Nwankwo, "Are Current Models of Data Protection Fit for Purpose?"
[39] Lehuedé, "Corporate Governance and Data Protection in Latin America and the Caribbean."
[40] Davis, "Data Protection in Africa: A Look at OGP Member Progress," 23.

### Equilíbrio entre o crescimento institucional e a supervisão regulatória

Assim que a APD for legalmente criada, os reguladores poderão enfrentar desafios para equilibrar o trabalho organizacional de estabelecer a instituição reguladora com o trabalho legalmente exigido de supervisão da proteção de dados. Como observou um agente da sociedade civil trabalhando em estreita colaboração com a proteção de dados na América Latina, os reguladores da APD "não têm tempo para criar a própria instituição [...] e para acompanhar o trabalho [que] são obrigados legalmente a fazer, que é investigar essas questões, investigar problemas, liberar recomendações". Um acadêmico africano e ativista da sociedade civil ecoou essas preocupações sobre a APD de seu país:

> Eles estão recrutando pessoal e construindo uma estrutura, e isso está acontecendo ao mesmo tempo em que se espera que eles comecem a trabalhar. Não há tempo para processar ou dizer: "Estamos nos consolidando como instituição". [...] A proteção de dados exige que eles estejam aplicando ou cumprindo o mandato que lhes foi concedido por lei, mas a instituição ainda é muito imatura, e o tema da proteção de dados está se desenvolvendo, está evoluindo.

Para novas APDs, o trabalho de construção de capacidade institucional e de início do cumprimento da lei geralmente ocorre de maneira simultânea. Um regulador de dados africano descreveu sua abordagem para a criação de uma APD enquanto enfrentava a falta de clareza legislativa sobre a estrutura organizacional e capacidade insuficiente:

> Nomeamos apenas nós cinco sem nada, apenas um orçamento de aproximadamente US$ 3,5 milhões, sem funcionários. Começamos literalmente do zero [...] A parte de proteção de dados foi bem difícil. Começamos fazendo o que chamamos de "visitas de estudo" a organizações semelhantes. Fomos ao Canadá, ao Reino Unido e à Alemanha. Depois disso, nós cinco nos reunimos e dissemos: "Como criaremos essa organização?" Éramos advogados. [...] Como não tínhamos dinheiro, não conseguíamos nem contratar consultores. [...] Nós criamos a estrutura organizacional. [...] Entrevistamos pessoas. Começamos com a camada superior, composta pelo Diretor-Presidente e pelos membros executivos. [...] Tivemos que trabalhar muito. Agora temos uma organização com 80 funcionários, temos um orçamento.

Para as novas APDs, o trabalho prático de definição da estrutura organizacional, contratação de pessoal, obtenção de orçamento e expansão da capacidade acontece juntamente com a supervisão da proteção de dados. Consequentemente, as comissões recém-criadas geralmente enfrentam restrições significativas para o cumprimento dos regulamentos e a garantia da conformidade. Como um agente da sociedade civil da África apontou, "inventar leis e decorar nossos marcos regulatórios com leis muito boas não é o bastante. É necessário dar um passo adiante e colocar em prática os princípios

de proteção de dados. E esse é o nosso maior problema." As próximas seções analisam esses desafios com mais detalhes.

## Financiamento e capacidade adequados

As restrições de financiamento são um grande obstáculo para as APDs no Sul Global.[41] Como exemplo, em 2018, o orçamento médio da APD por país africano foi de US$ 500.000 com 14 funcionários e de US$ 400.000 por país latino-americano com 13 funcionários, em comparação com US$ 58 milhões e 647 funcionários por país na América do Norte.[42] Como observou Teki Akuetteh Falconer, fundadora e diretora executiva do Africa Digital Rights' Hub e ex-reguladora de dados do Gana, "A principal questão não é se os países têm as leis 'certas' ou as instituições 'certas' em vigor, [mas] se eles têm os recursos necessários para implementar as leis existentes com eficácia".[43] Embora os governos do Sul Global priorizem cada vez mais a supervisão da proteção de dados, as APDs devem competir por financiamento com outras prioridades estaduais, como segurança nacional e desenvolvimento de infraestrutura. Como afirmou um entrevistado que representa uma APD africana, "a provisão de recursos é mais destinada à saúde por causa da COVID ou a muitas outras prioridades, como o desenvolvimento de infraestrutura". Entre elas, como enfatizaram os participantes da mesa redonda, a pandemia de COVID-19 precipitou restrições orçamentárias significativas da APD, à medida que os governos realocavam fundos para os ministérios da saúde.

A estrutura e o mandato de uma APD também afetam o financiamento. Por exemplo, apesar de seus benefícios de cumprimento e harmonização, os mandatos duplos podem sobrecarregar os recursos operacionais, como observou um participante da mesa redonda. Outro entrevistado de uma APD africana argumentou que, como seu órgão de proteção de dados estava estruturado em outra agência, "o orçamento é muito limitado porque [as autoridades públicas] analisam nosso orçamento como um todo. [...] Elas vão segregá-lo e dizer que é para o órgão. Mas por causa de tantas prioridades conflitantes, não teremos recursos suficientes." No entanto, outro entrevistado disse que fazer parte de uma organização controladora protegeu sua APD de cortes significativos de financiamento, principalmente em suas etapas iniciais e durante a pandemia global. Em muitas jurisdições, as preocupações com o financiamento também são agravadas pela incapacidade das APDs de cobrar multas consideráveis e, às vezes, pelos meios para cobrá-las. Além disso, em alguns casos, as disposições legais proíbem as APDs de cobrar multas e usá-las para seu orçamento, direcionando-as ao tesouro. Da mesma forma,

[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), janeiro de 2018), https://iapp.org/media/pdf/resource_center/DPA-Budget-Staffing-Whitepaper-FINAL.pdf.
[43] Pisa e Nwankwo, "Are Current Models of Data Protection Fit for Purpose?," 2.

algumas APDs só têm o poder de cobrar sanções criminais em vez de multas administrativas porque, como afirmou um regulador da África, "o governo está preocupado com o abuso desse poder".

Os desafios de financiamento inevitavelmente restringem as atividades das APDs. Orçamentos inadequados restringem os esforços de recrutamento de pessoal, afetando a capacidade das agências e as funcionalidades de investigação. Um regulador da África que enfrenta restrições de recursos explicou que

> em termos de recursos humanos, você é muito limitado. Temos uma estrutura de aproximadamente 35 [funcionários e], em termos de pessoas com contratos de prazo bastante longo, temos cerca de três. Conseguimos contratar alguns funcionários temporários para ajudar [...], mas os seus contratos também são muito curtos. Em termos de recursos humanos, de ferramentas, de capacidade de garantir a conformidade, isso é um desafio quando os recursos são limitados.

Assim como nas agências reguladoras na Europa e na América do Norte, as APDs geralmente competem com o setor privado com muito mais recursos por especialistas em proteção de dados, colocando as agências em desvantagem.[44] O fenômeno da "fuga de cérebros", principalmente a migração de especialistas para mercados mais lucrativos, muitas vezes não regionais,[45] intensifica essa desvantagem. Além de restringir a capacidade de pessoal das APDs, as restrições de recursos afetam a capacidade das agências de realizar funções básicas. Por exemplo, vários reguladores declararam que estabelecer um registro para controladores e operadores de dados – essenciais para manter a transparência e a responsabilidade – sobrecarregava APDs com poucos recursos e redirecionava a atenção da tarefa crucial de cumprimento e monitoramento da conformidade. Da mesma forma, as APDs recém-criadas e subfinanciadas lutam para conscientizar o público sobre as leis de proteção de dados, o que é fundamental não apenas para estabelecer a conformidade, mas também para o cumprimento por meio de litígios civis. Como um regulador enfatizou, essas campanhas podem ser caras, pois as mensagens públicas não apenas devem ser criadas, mas também lançadas repetidamente por vários canais para garantir que cheguem aos setores público e privado.

## Garantia da Independência

A independência regulatória de uma APD é essencial para sua legitimidade, responsabilidade e eficácia.[46] Vários fatores inter-relacionados compõem essa

[44] Pisa e Nwankwo, "Are Current Models of Data Protection Fit for Purpose?"
[45] Mannion, "Data Imperialism."
[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 maio de 2018), https://www.internetsociety.org/resources/doc/2018/personal-data-protection-guidelines-for-africa/.

independência. Os fatores estruturais estão relacionados à forma como uma APD é criada, incluindo se ela está situada dentro de agência e é responsável por essa última. Os fatores de divulgação de informações estão relacionados à governança da APD, principalmente qual entidade supervisiona a agência e se ela pode anular as decisões da APD. As considerações orçamentárias ou econômicas envolvem quem controla o orçamento de uma APD, incluindo preocupações sobre o armamento desse controle, ameaçando o financiamento para enfraquecer o cumprimento.[47] Juntos, esses fatores podem minar a independência institucional e adjudicatória de uma APD, pois a primeira está relacionada a questões operacionais, como financiamento, e a última denota independência na tomada de decisões.[48]

Muitas APDs na África e na América Latina lutam para alcançar a independência de agentes públicos e privados, o que prejudica sua capacidade de cumprimento. Elas são especialmente vulneráveis a ameaças à independência dos governos que as criam e financiam. As razões oficiais para a construção de dependências orçamentárias e de tomada de decisão na estrutura de uma APD são diversas. Por exemplo, um ex-regulador latino-americano de proteção de dados observou que a justificativa oficial para a estruturação inicial da APD do país sob a égide do Ministério da Justiça, e não como uma agência independente, era que "um novo órgão com um orçamento independente [...] criará mais problemas para o orçamento nacional, [já que o país] não estava em uma situação econômica e financeira muito boa." Essa estrutura prejudicou bastante a independência da APD e a agência só foi reformada anos depois. Da mesma forma, um representante da sociedade civil ofereceu um exemplo ilustrativo das ameaças estruturais e financeiras a uma APD africana:

> Nossa autoridade reguladora está meio que fundida em um ministério, subordinado à presidência. Portanto, ele não permitiu [à APD] nenhum tipo de independência. Ela não tem independência estrutural ou financeira. Mesmo se o regulamento ou a legislação fosse bem-intencionada, ela sempre está de mãos atadas. Aqueles que estão no conselho também fazem parte do governo. O chefe da organização é [...] nomeado pelo presidente, de modo que não há espaço de manobra para que [os reguladores] se oponham em termos de cumprimento, o que é um grande problema, pois os maiores operadores de dados [no país] são o governo.

Mesmo países com fortes registros de proteção de dados enfrentam essas restrições estruturais. Por exemplo, a APD do Brasil tem independência limitada do presidente, que tem controle sobre seu orçamento. Além disso, três dos cinco membros do conselho da APD são autoridades militares. Esses obstáculos estruturais prejudicam as funções diárias e as capacidades de cumprimento das APDs, principalmente quando o governo

[47] Davis, "Data Protection in Africa: A Look at OGP Member Progress."
[48] Ibid., 50.

ou outra agência controla o orçamento da APD. Os entrevistados também enfatizaram o papel de limites de prazo restritos para reguladores e procedimentos de renomeação não transparentes para minar a legitimidade e a independência das APDs. Um regulador latino-americano enfatizou fatores estruturais como a incapacidade de uma APD de modificar a política pública em meio a novos desenvolvimentos de proteção de dados, com o objetivo de minar a independência judicial.

Dadas as significativas restrições de recursos enfrentadas por muitas APDs, vários participantes da mesa redonda enfatizaram a importância da "independência econômica" ou orçamentária, ou seja, estabilidade e consistência financeiras. Como afirmou um regulador africano, "se não tivermos um orçamento adequado, dificilmente conseguiremos mostrar nossa independência". No entanto, muitos participantes viram seu financiamento da APD realocado ou cortado pelos governos durante a pandemia da COVID-19, à medida que o trabalho remoto se proliferava, aumentando a probabilidade de abusos na proteção de dados. Da mesma forma, enquanto alguns participantes observaram que estar inserido em outro órgão regulador pode proteger uma APD contra ameaças ao seu orçamento, outros observaram o contrário, incluindo restrições de financiamento impostas pela agência controladora.

As restrições à independência da APD na África e na América Latina decorrem não apenas da escassez de recursos, mas também porque o regulamento da proteção de dados pode invadir a atividade do setor público. Como Kuda Hove, da Privacy International, observou a respeito de alguns governos na África:

> Há uma desconfiança geral em relação às instituições independentes [...] Há uma desconfiança [de que] se lhes dermos verdadeira autonomia, verdadeira independência, elas podem se voltar contra nós no futuro, essa é a opinião dos governos. Portanto, para gerenciar esse receio, eles vão minar a independência.[49]

Por exemplo, um pesquisador observou que, na África do Sul, a criação de "agências independentes nunca se mostrou atraente para os ministros do ANC [partido majoritário], que preferem manter o controle",[50] resultando em uma implementação lenta da legislação de proteção de dados e sua avaliação. Além disso, a legislação de proteção de dados geralmente dá aos ministros o poder de criar isenções legais, revisar regulamentações e intervir nas atividades de cumprimento, tornando as APDs vulneráveis à captura regulatória.[51] Por exemplo, o NDPR (Regulamento de Proteção de Dados da Nigéria) pode ser revogado por qualquer ato do Parlamento, e a agência reguladora da Nigéria, NITDA (Agência Nacional de Desenvolvimento de Tecnologia da Informação), tem um mandato significativamente limitado, incluindo a falta de poder

[49] Ibid.
[50] Sutherland, "The Governance of Data Protection in South Africa," 14.
[51] Ademuyiwa e Adeniran, "Assessing Digitalization and Data Governance Issues in Africa."

discricionário de cumprimento.[52] Da mesma forma, as leis de proteção de dados da maioria dos países latino-americanos isentam as agências policiais e de inteligência estaduais, como Brasil, Peru e Panamá.[53]

No entanto, os agentes do setor público estão entre os abusadores prolíficos da proteção de dados pessoais.[54] Por exemplo, autoridades eleitorais do Quênia supostamente coletaram e usaram indevidamente dados biométricos durante as eleições de 2017.[55] Da mesma forma, várias agências nigerianas coletaram grandes quantidades de dados públicos como condição para a emissão de documentos importantes do estado, como carteiras de motorista e passaportes. Casos semelhantes de violações de privacidade governamentais deliberadas ou acidentais surgiram em países como Gana e África do Sul.[56] Na América Latina, um regulador de dados informou que "o governo federal [está] usando a lei geral de proteção de dados [do país] para negar o acesso às informações". Enquanto isso, outros governos da região se isentaram das leis de proteção de dados em suas atividades de manuseio e tratamento de dados, incluindo aplicativos de rastreamento de contatos.[57] Como relatou um representante da sociedade civil:

> Sabemos que tudo o que ocorre no setor público, especificamente relacionado ao poder executivo, ficará ainda mais difícil de ser investigado, ou haverá uma investigação branda. [...] Por exemplo, o poder executivo e a Polícia Federal estão tentando comprar sistemas biométricos. E nós, em coalizão de outras organizações, denunciamos isso, e [...] as autoridades disseram: 'Não, está tudo bem, pode contar conosco.'

Outro representante latino-americano argumentou que essa falta de independência geralmente acarreta procedimentos regulatórios não transparentes. O entrevistado observou que, devido à proximidade do governo em questão com o setor privado, os representantes da APD se reúnem ocasionalmente com uma empresa sob investigação, mas não convidam membros da sociedade civil e mantêm o processo escondido do público. Representantes da sociedade civil afirmaram que, na maioria das vezes, não conseguiam obter uma resposta dos reguladores, agendar reuniões com eles ou acessar documentos legais pertinentes às investigações. Essa opacidade processual, por sua vez, faz com que seja difícil identificar se uma APD deixa de realizar uma investigação específica devido a restrições de recursos ou a interesses políticos e alianças conflitantes. Consequentemente, mesmo que elas tenham origem no próprio governo

[52] Bryant, "Africa in the Information Age."
[53] Rodriguez e Alimonti, "A Look-Back and Ahead on Data Protection in Latin America and Spain."
[54] Bryant, "Africa in the Information Age."
[55] Ibid.
[56] Ibid.
[57] Javier Pallero, "Collective Challenges and Opportunities in Data Protection: A Latin American Perspective," Luminate, 26 de maio de 2021, https://luminategroup.com/posts/blog/collective-challenges-and-opportunities-in-data-protection-a-latin-american-perspective.

na maioria dos casos, as ameaças à independência das APDs também podem afetar as investigações no setor privado.

## Conformidade e Conscientização

A implementação e o cumprimento de leis de proteção de dados pressupõe um grau de alfabetização digital pública, por exemplo, para obter o consentimento informado dos usuários antes da coleta de dados.[58] Da mesma forma, a conformidade do setor privado com a lei exige que as empresas estejam familiarizadas com as leis e os regulamentos existentes. Ambas as condições apresentam desafios para as APDs, principalmente em países com baixa alfabetização digital e difusão tecnológica. Embora a conscientização sobre questões de privacidade tenha aumentado nos últimos anos – por exemplo, conforme evidenciado por um aumento de 20 a 30% nas reclamações de privacidade apresentadas às APDs africanas[59] – o problema persiste entre a população em geral. Por exemplo, pesquisas em Gana descobriram que os usuários da Internet não estavam familiarizados com questões de privacidade e proteção de dados e muitas vezes desconheciam seus direitos de privacidade ou o que fazer se esses direitos fossem violados.[60] A pesquisa também descobriu que, para muitas pessoas, a privacidade não era uma prioridade.[61] Como disse um participante da mesa redonda, um dos principais desafios é "a falta de conscientização [tanto] em termos de os titulares conhecerem seus direitos quanto dos controladores de dados conhecerem suas obrigações". Vários outros participantes argumentaram que a conscientização é uma prioridade significativa para as APDs na África e na América Latina.

Informar o público sobre privacidade e proteção de dados é fundamental para a capacidade das APDs de cumprir efetivamente seus mandatos. A falta de familiaridade do público com as leis de privacidade prejudica não apenas a possível aplicação da responsabilidade civil, mas também o exercício dos direitos básicos dos cidadãos, como direitos de acesso, correção ou exclusão de seus dados.[62] Além disso, a baixa alfabetização digital, associada à conscientização limitada sobre privacidade, poderá minar os esforços das APDs para aumentar a transparência em relação às questões de proteção de dados (por exemplo, desenvolvendo um registro público de dados) e a legitimidade pública das agências. Em muitos casos, como observou um entrevistado da África, as leis de proteção de dados devem ser traduzidas do inglês para o idioma local e simplificadas "para que a população possa entender o que ela ganha com isso" quais são os benefícios de ter seus dados pessoais protegidos". O entrevistado enfatizou que

[58] Pisa e 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] Ibid.
[62] Davis, "Data Protection in Africa: A Look at OGP Member Progress."

a conscientização do público é um processo de longo prazo e que demanda muitos recursos:

> [R]ecursos para preencher as lacunas de recursos humanos e criar a conscientização são muito importantes. Na minha opinião, para você atingir essa população [que não tem conhecimento das leis de proteção de dados], é necessário propagar essa mensagem várias vezes, quase toda semana, ou com frequência. E esse espaço midiático leva tempo. Você precisa de pessoas para desenvolver esse conteúdo. Você precisa pagar para que sua mensagem seja transmitida.

Consequentemente, as restrições de recursos podem prejudicar os esforços para aumentar a conscientização pública sobre as leis de proteção de dados, o que, por sua vez, pode intensificar os desafios relacionados ao cumprimento e à conformidade da APD.

Da mesma forma, o desconhecimento dos operadores e controladores de dados dos setores público e privado com as leis locais de proteção de dados pode prejudicar a conformidade e sobrecarregar os esforços de cumprimento. Como exemplo, apesar da aprovação da legislação de proteção de dados na África do Sul em 2013, muitas empresas nacionais e estrangeiras não a cumprem, e as violações de dados provavelmente são subnotificadas.[63] Essa taxa de descumprimento cresceu com a difusão de tecnologias com uso intensivo de dados, como smartphones.[64] Além disso, apesar de anos para o cumprimento da nova lei, pesquisas revelam que apenas 25% dos sites mais populares do país pedem aos usuários consentimento para coletar seus dados.[65] Da mesma forma, os pesquisadores descobriram que alguns sites do governo de Ruanda não cumpriram os princípios básicos de proteção de dados, como ter uma política de privacidade.[66] Um operador de site acreditou por engano que a proteção de dados está enraizada na lei tributária, enquanto outro afirmou que "[n]ão há política a ser seguida; Eu [gerencio as informações pessoais] seguindo meu bom senso."[67] O setor público não está imune ao baixo cumprimento e, em alguns casos, é um infrator ainda pior do que o setor privado. Depois de exigir que os controladores de dados se registrem em um registro público criado recentemente, um regulador africano de proteção de dados observou:

> Percebemos, por exemplo, que, os setores financeiro e de seguros são muito complacentes. Estamos vendo hospitais e clínicas começando a se registrar. Isso

[63] Sutherland, "The Governance of Data Protection in South Africa."
[64] Ibid.
[65] Bryant, "Africa in the Information Age."
[66] Chantal Mutimukwe, Ella Kolkowska e Åke Grönlund, "Information 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.
[67] Ibid., 8.

está melhorando, mas onde notamos baixas taxas de conformidade é dentro do governo. Talvez isso aconteça porque eles não estão cientes das leis.

Consequentemente, os controladores e operadores de dados do setor público podem apresentar os maiores desafios à conformidade e uma prioridade fundamental para as campanhas de conscientização das APDs sobre as leis de proteção de dados.

## Cumprimento

Embora seja uma de suas responsabilidades mais fundamentais, muitas APDs na África e na América Latina enfrentam desafios significativos no cumprimento efetivo das leis de proteção de dados. Eles decorrem, em parte, de mandatos de cumprimento pouco claros e excessivamente limitados e de isenções legais ambíguas.[68] Por exemplo, a APD da Nigéria, NITDA, não tem um poder de fiscalização claro.[69] Outro obstáculo premente, e um tema-chave na mesa redonda, é a ausência de pessoal especializado e financiamento para investigar casos e abusos. Ao mesmo tempo, avaliar as atividades de cumprimento das APDs é difícil devido aos dados inconsistentes sobre investigações em todas as jurisdições. Por exemplo, muitas APDs africanas não divulgam suas ações de cumprimento, embora países como África do Sul e Gana tenham perseguido ativamente as empresas que não as cumprem, sendo que esse último instituiu um tribunal de tramitação rápida para processar os infratores.[70]

Três desafios de cumprimento relacionados envolvem medidas punitivas. Em primeiro lugar, muitos tribunais africanos carecem de experiência judicial em questões de proteção de dados, agravada pela insuficiência de jurisprudência sobre privacidade na região.[71] Tribunais inexperientes podem prejudicar o cumprimento, principalmente em ações de responsabilidade civil.[72] Por outro lado, como foi documentado na Nigéria, quando o público não está familiarizado com os direitos de privacidade locais, as pessoas raramente instauram processos contra os infratores, dando aos tribunais poucas oportunidades de desenvolver expertise e jurisprudência sobre proteção de dados.[73] Da mesma forma, muitos tribunais africanos sofrem com atrasos significativos e desconfiança pública, o que contribui para a reticência das pessoas em buscar recursos legais.[74] Para APDs que podem impor apenas sanções criminais e não financeiras, um sistema judicial sobrecarregado pode frustrar o cumprimento. Como um regulador

[68] Davis, "Data Protection in Africa: A Look at OGP Member Progress"; Rodriguez e Alimonti, "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 e 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 e Adeniran, "Assessing Digitalization and Data Governance Issues in Africa."
[71] Davis, "Data Protection in Africa: A Look at OGP Member Progress."
[72] Ibid.
[73] Abdulrauf e Fombad, "Personal Data Protection in Nigeria."
[74] Mannion, "Data Imperialism."

africano apontou, embora os governos possam estar relutantes em permitir que as APDs emitam multas administrativas por preocupação com o abuso de poder, a alternativa geralmente é postergada ou não é cumprida.

Em segundo lugar, para as APDs que podem buscá-las, as sanções administrativas para os infratores variam amplamente entre as jurisdições. Por exemplo, de acordo com a LGPD brasileira, as multas podem chegar a dois por cento do valor bruto anual de uma empresa ou conglomerado econômico,[75] enquanto em Gana, a multa mais alta é de aproximadamente US$ 10.500.[76] Como mecanismo de dissuasão, muitas sanções não são consideradas fortes o bastante.[77] Ações limitadas de cumprimento, juntamente com sanções ineficazes, correm o risco de cultivar uma cultura de impunidade.[78] Essas pequenas multas são malsucedidas principalmente na punição de grandes empresas estrangeiras infratoras.

Assim, um terceiro desafio de cumprimento relacionado envolve a instauração de processos contra empresas estrangeiras, geralmente big techs. Embora os marcos de privacidade europeus e norte-americanos geralmente ofereçam proteção para fluxos de dados transnacionais envolvendo seus cidadãos, big techs de países como EUA e China coletam e tratam dados de muitos países do Sul Global, muitas vezes com impunidade.[79] Um estudo descobriu que subsidiárias de empresas de telecomunicações europeias que atuam no Senegal e no Quênia não ofereceram aos africanos os mesmos direitos de dados que suas controladoras concedem aos europeus.[80] Como disse um participante da mesa redonda, "quando enfrentamos grandes empresas que não estão sediadas em nossos países, é difícil fazer a investigação e, no fim das contas, é difícil garantir a execução da decisão". Outro entrevistado da América Latina destacou como a falta de cumprimento das leis locais, associada aos mecanismos de sanção insuficientes, prejudicou as ações de cumprimento contra big techs:

> Se eu decidir um caso contra o Google, por exemplo, a resposta usual do Google é: "Suas leis não se aplicam a mim". [...] E mesmo quando o tribunal disse: "Sim, essa lei se aplica a você, você tem que pagar a multa", ou o que quer que seja, às

[75] Lehuedé, "Corporate Governance and Data Protection in Latin America and the Caribbean," 39.
[76] Ademuyiwa e Adeniran, "Assessing Digitalization and Data Governance Issues in Africa."
[77] Ibid. 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 e Charlotte Lenz, "Data Extraction by Chinese Phone Applications in Africa: An Analysis of Risks and Regulatory Protection," Oxford China International Consultancy, 6 de maio 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 maio de 2021, sec. África, https://www.reuters.com/world/africa/south-african-regulator-seeking-legal-advice-whatsapps-new-privacy-policy-2021-05-13/.
[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 Without Borders, janeiro de 2018), https://www.accessnow.org/cms/assets/uploads/2018/02/RDR-Africa_Final-version-5_January-2018.pdf.

> vezes é complicado garantir o cumprimento das decisões. [...] O outro problema é que [...] o valor das multas é muito baixo quando você converte em dólares neste momento [...] É mais barato pagar a multa, se eles quiserem pagar, do que fazer as mudanças estruturais que precisam ser feitas para respeitar a lei.

O desafio de cumprimento das leis locais de proteção de dados contra violações estrangeiras levanta questões sobre a legitimidade internacional das APDs. Além disso, como essas ações de cumprimento geralmente falham, as APDs geralmente se concentram em empresas nacionais,[81] o que pode impedir a inovação local e minar a competitividade internacional das empresas de tecnologia locais.

Além dos obstáculos relacionados a sanções, uma preocupação premente é a falta regional de consultores técnicos especializados. O desafio afeta tanto a África quanto a América Latina e pode complicar as ações de cumprimento. Como disse um ex-regulador latino-americano:

> Se quiser investigar seriamente [uma] violação de dados, você precisa de bons cientistas ou engenheiros da computação que possam acessar os registros e ver exatamente se eles estavam respeitando as garantias básicas para proteger dados pessoais ou não. Isso é muito difícil de entender ou fazer se você for um advogado. Portanto, é necessário ter um departamento específico, um grupo específico de pessoas, investigadores, que são técnicos. E isso é um problema, porque na América Latina e também na Europa, até onde eu sei, é muito complicado contratar gente boa por causa do salário dos técnicos, das pessoas que trabalham na informática, na segurança das redes. Nesse tipo de atividade, geralmente [...] as pessoas são muito bem pagas e não querem ser [membros de] uma Autoridade de Proteção de Dados. [...] Claro que o problema será muito pior se o seu orçamento for baixo. Se você não tiver o próprio orçamento, a dificuldade será muito pior. Mas mesmo quando você tem um orçamento, isso é um problema.

A falta de recursos e os salários mais baixos do setor público impedem o recrutamento de especialistas locais e, quando combinados com tribunais inexperientes, podem dificultar investigações completas e impedir a aplicação de sanções.

Finalmente, as ameaças à independência da APD também podem prejudicar o cumprimento. Um defensor da sociedade civil africana salientou que o governo do país não quer que a APD processe o setor público. Consequentemente,

> até o momento, todos os esforços [de cumprimento] estão voltados para as empresas. Mesmo assim, eu não diria que isso é muito eficaz. [Desde a criação da autoridade, alguns anos antes] houve dois ou três processos e não há um

[81] Pisa e Nwankwo, "Are Current Models of Data Protection Fit for Purpose?"

> [número] preciso de quantas pessoas estão violando as leis de proteção de dados.

Em última análise, essa supervisão de proteção de dados fragmentada corrói a legitimidade de uma APD e, por extensão, sua capacidade de cultivar a familiaridade pública e privada com os direitos e responsabilidades dos dados.

## Problemas de política emergentes

Sistemas tecnológicos estabelecidos, mas em proliferação, como a Internet das Coisas (IoT), a adoção cada vez maior de tecnologias blockchain e computação descentralizada e os avanços em Inteligência Artificial (IA) trazem implicações para o regulamento de privacidade e proteção de dados.[82] Por exemplo, os requisitos de exclusão modelados após o GDPR são anteriores e não podem ser aplicados com facilidade aos registros imutáveis que caracterizam as blockchains.[83] Os sistemas de IA permanecem praticamente não regulamentados em vários países africanos,[84] e os esforços dos formuladores de políticas para avaliar as abordagens regulatórias para tecnologias emergentes têm sido lentos.[85]

A proliferação de smartphones, IoT e processamento em nuvem complica bastante os fluxos de dados transnacionais, levantando questões legais importantes sobre a obtenção de consentimento e sobre como alcançar a harmonização regulatória em meio a diversas regras nacionais de proteção de dados que esses fluxos de dados implicam.[86] Poucos países africanos têm regras claras sobre esses fluxos,[87] cuja definição será cada vez mais premente. No entanto, discursos políticos que simplesmente assumem a utilidade social e os benefícios econômicos das tecnologias emergentes servem como um obstáculo ao desenvolvimento dessas regras. Como um defensor da sociedade civil africana enfatizou:

> Parece que temos uma tendência de adotar as tecnologias [...] pela conveniência que elas trazem. E, na maioria dos casos, a mensagem sobre a conveniência da tecnologia supera as preocupações relacionadas à privacidade. Neste momento, há uma conversa sobre a Quarta Revolução Industrial, sabe, 'Precisamos fazer parte do mundo desenvolvido', 'Você precisa adotar essa tecnologia'. Mas a conversa sobre proteção de dados de privacidade se perdeu ao longo do caminho. [...] E [nosso país] pretende adotar um sistema de identificação biométrica mais avançado e mais centralizado. E vai ser muito fácil acessar

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

informações sobre uma pessoa, mas onde está a conversa sobre a proteção dessas informações, que são muito confidenciais?

Além disso, como vários entrevistados apontaram, muitas APDs na região priorizam necessariamente a capacitação, ocupando a maior parte do foco e do tempo dos reguladores de proteção de dados. No entanto, como observou um regulador, algumas APDs africanas estão adotando abordagens proativas e desenvolvendo novos marcos de políticas, como para tecnologias controladas por IA e para fintech.

Na América Latina, o desenvolvimento de regulamentos para tecnologias emergentes também é desigual. Alguns países se concentraram no desenvolvimento de marcos para questões políticas emergentes. Por exemplo, Barbados e El Salvador adotaram tecnologias como criptomoedas como parte de seu plano nacional de desenvolvimento.[88] No entanto, novas preocupações políticas continuam se materializando, inclusive em torno da regulação dos sistemas de identidade digital[89] e da digitalização dos dados de DNA pertencentes a pessoas físicas.[90] As APDs precisarão definir a supervisão dessas atividades com uso intensivo de dados. Além disso, como os atores da sociedade civil da região argumentaram, a fiscalização existente ainda precisa conter problemas familiares, como violações de dados, fraude bancária, preocupações relacionadas à segurança cibernética em torno dos sistemas de cartão de crédito, bem como supervisão insuficiente de novas tecnologias de IA. Como declarou um representante da sociedade civil, "a tendência é que [esses problemas] aumentem, já que nada está sendo feito sistematicamente para enfrentá-los". A realidade política incerta testemunhada por vários países na região, conforme vários entrevistados demonstraram, apenas aumenta os desafios de capacidade das APDs quanto à supervisão de novas tecnologias e às respectivas questões de proteção de dados.

## Colaboração com outras APDs, agências reguladoras e sociedade civil

A colaboração entre as APDs regionais, com outras instituições reguladoras nacionais e com a sociedade civil pode aumentar a capacidade e a eficácia das atividades diárias das APDs – desde a conscientização até a realização de investigações eficientes e completas. Uma maior colaboração e coordenação regional entre APDs, especialmente útil para agências recém-criadas, pode permitir o compartilhamento de melhores práticas e reforçar as ações de cumprimento contra empresas que operam de maneira transnacional.[91] A parceria com outros órgãos reguladores nacionais, como agências de proteção ao consumidor e reguladores setoriais, pode aprimorar as investigações de fiscalização e aumentar a conformidade. Trabalhar com a sociedade civil pode cultivar a conscientização pública sobre questões de proteção de dados, aumentar a

[88] Martins de Almeida, "Data Protection in Latin America."
[89] Ibid.
[90] Sutherland, "The Governance of Data Protection in South Africa."
[91] Pisa e Nwankwo, "Are Current Models of Data Protection Fit for Purpose?"

responsabilidade e a legitimidade das APDs e ajudar na identificação de violações. Apesar dos diversos benefícios, essas alianças também enfrentam desafios, na maioria das vezes relacionados a objetivos e mandatos divergentes e diferenças culturais ocasionais.

### Colaboração com outras APDs

A colaboração regional entre as APDs tem sido fundamental para estabelecer novas agências e desenvolver suas capacidades. Por exemplo, uma participante da mesa redonda da África contou como ela e sua equipe visitaram agências de proteção de dados em vários países do Norte Global para desenvolver um plano para a APD em seu país de origem. No entanto, outro entrevistado afirmou que as parcerias com APDs do Norte Global são muito raras. Em vez disso, a colaboração é mais frequente no âmbito regional, onde o compartilhamento das melhores práticas é uniforme, se não mais útil. Um regulador africano relatou várias maneiras pelas quais essas colaborações reforçam a proteção de dados nacionais:

> Quando falo com meu colega na África do Sul, sim, levou tempo para eles chegarem aonde estão, mas agora eles estão totalmente financiados. Seus níveis de conformidade estão aumentando. Então, vamos discutir, como eles fizeram isso? Será que eles podem oferecer algumas dicas? Compartilhamos marcos como seus documentos estratégicos. Atualmente, estamos criando nosso plano estratégico, mas recebemos planos estratégicos da África do Sul, do Quênia, de Gana, então compartilhamos esses documentos. [...] Também compartilhamos algumas dessas documentações [regulamentares] que são úteis, principalmente para nós, pois talvez não consigamos contratar consultores imediatamente para fazer esse trabalho para nós [de redigi-los]. [...] A colaboração é muito importante. Isso já está ocorrendo dentro dos comissários de proteção de dados. E acho que só podemos melhorar, mas é algo que todos reconhecemos que é necessário para nós.

Além de compartilhar as melhores práticas e os documentos regulatórios, alguns entrevistados que estão criando sua capacidade de APD também relataram a comparação de seu progresso com outras agências da região.

A parceria com APDs regionais também pode fortalecer a capacidade coletiva de influenciar big techs estrangeiras. Como afirmou Thelma Quaye, da SmartAfrica, "se os países africanos apresentarem uma frente unida na política de dados, como os Estados-Membros da UE, eles teriam maior poder para influenciar e mudar o comportamento dessas empresas".[92] Por exemplo, a atualização da política de privacidade da Meta de março de 2021 para o WhatsApp, que anunciou que o serviço de mensagens compartilharia dados do usuário nos serviços da controladora, incluindo o Facebook,

[92] Ibid., 2.

violou a POPIA (Lei de Proteção de Informações Pessoais), a lei sul-africana de proteção de dados.[93] A APD do país encaminhou a questão para a Assembleia Global de Privacidade, da qual é membro, para pressionar a Meta a cumprir sua lei.[94] Como disse um entrevistado,

> Somos muito pequenos, por isso pensamos que, se nos ocuparmos deste assunto como Assembleia Global de Privacidade, certamente teremos um rumo. Ainda estamos conversando com a assembleia sobre a abordagem que devemos escolher, mas acho que essas são algumas das questões. Se estivermos lidando com um grande player como WhatsApp ou Facebook, será importante para nós, como Autoridades de Proteção de Dados no mundo, nos unirmos na tentativa de forçar grandes players como esse a estar em conformidade.

Além de aumentar a capacidade de cumprimento contra big techs, a colaboração regional também costuma ser um pré-requisito para investigações eficazes, principalmente devido à natureza cada vez mais internacional dos fluxos de dados. Como afirmou um ex-regulador latino-americano:

> Hoje, quando você quer investigar alguma [...] violação da lei em termos de proteção de dados, é altamente possível que você precise investigar algo que [também] ocorre em outro país. Portanto, é necessário ter cooperação de outras agências que estão em outro país também. [...] Se você vê o que está acontecendo na Europa, digo, em termos do GDPR, as diferentes APDs colaboram. O problema na América Latina é que queremos colaborar, mas colaboração não é algo que está acontecendo neste momento. Sendo assim, é muito difícil investigar as violações de proteção de dados pessoais quando você não tem a possibilidade de investigar ou obter alguma evidência que está no exterior.

Essas observações também se estendem à África, onde muitas economias regionais estão fragmentadas e têm pequenos mercados. Consequentemente, as empresas regionais de tecnologia têm incentivos para expandir as operações além das fronteiras nacionais.[95] No entanto, as regulamentações de proteção de dados em toda a região são inconsistentes, estipulando regras diferentes para acesso às informações do usuário, exclusão e notificações de violação de dados e exigindo proteções diversas para dados confidenciais.[96]

[93] Reuters, "South African Regulator Seeking Legal Advice on WhatsApp's New Privacy Policy."
[94] Duncan McLeod, "South Africa Threatens Litigation over New WhatsApp Privacy Policy," TechCentral, 14 de maio de 2021, https://techcentral.co.za/south-africa-threatens-litigation-over-new-whatsapp-privacy-policy/170079/.
[95] Ademuyiwa e Adeniran, "Assessing Digitalization and Data Governance Issues in Africa."
[96] Davis, "Data Protection in Africa: A Look at OGP Member Progress."

O cenário regulatório fragmentado pode aumentar os custos de conformidade para empresas que operam de maneira transnacional, o que cria incentivos para os reguladores africanos harmonizarem suas leis de proteção de dados.[97] A colaboração entre as APDs é fundamental para esse esforço. Durante a última década, os países africanos articularam vários marcos regionais de proteção de dados, incluindo a proeminente Convenção da União Africana sobre Segurança Cibernética e Proteção de Dados Pessoais de 2014, conhecida como Convenção de Malabo.[98] Incentivos adicionais para a harmonização vieram da Zona de Comércio Livre Continental Africana (AfCFTA), que promove a integração do mercado regional, a interoperabilidade e a garantia dos fluxos de dados regionais.[99] Como um regulador africano apontou, estabelecer um marco regional comum pode aumentar a conformidade e ajudar na busca de ações de cumprimento contra big techs: "Se concordarmos que 'Estes são os princípios que você deve cumprir' e garantirmos que [big techs] o façam em toda a região africana, essa colaboração também nos permite obter essa alavancagem que talvez [nossa APD] não seja capaz de assumir." No entanto, nem a Convenção de Malabo nem os outros marcos foram ratificados e a proteção de dados na África continua sendo predominantemente o domínio das leis e regulamentos nacionais.[100]

Esses esforços de harmonização são prejudicados pela ausência de uma infraestrutura jurídica abrangente, como a da UE, que poderia incentivar a implementação e aplicação da integração regional.[101] Além disso, a colaboração também é frustrada por conhecimentos técnicos e regulatórios inconsistentes em toda a região e, às vezes, por objetivos políticos e regulatórios contraditórios. Alguns reguladores podem preferir marcos de proteção de dados mais fortes ou diferentes do que seus colaboradores regionais, contribuindo para atritos ou divergências.[102] Apesar do desejo de colaborar e compartilhar experiências, os entrevistados também mencionaram as barreiras culturais e linguísticas como obstáculos ocasionais para parcerias efetivas, tanto entre regiões quanto dentro delas. Por exemplo, um regulador africano observou:

> Acho que os falantes de inglês se comportam de maneira diferente dos falantes de francês. Às vezes isso pode atrapalhar essa colaboração porque acho que, em alguns momentos, a gente não se entende muito bem. [...] Algumas coisas são muito burocráticas. Os anglófonos preferem estabelecer os princípios e permitir que as pessoas trabalhem. Os franceses definem os princípios, então eles querem passar por um período de treinamento para eles tomarem uma decisão [sobre os princípios]. Existem algumas diferenças.

[97] Pisa e 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] Ibid. Bryant, "Africa in the Information Age."
[101] Adeyoju, "Data Privacy Harmonisation in Africa."
[102] Ibid.

Além disso, em um nível prático, o trabalho com APDs regionais pode ser demorado e exigir uma coordenação significativa, que requer estrutura: as reuniões devem ser marcadas e acompanhadas, e seus objetivos devem ser definidos e monitorados. Como apontou um ex-regulador latino-americano, as redes colaborativas são tão fortes quanto os nós que as constituem e exigem confiança significativa para operar de maneira eficaz. Construir essa confiança pode ser um desafio, pois os reguladores que comandam as APDs variam. Organismos de coordenação regional, como a Red Iberoamericana de Protección de Datos (RIPD) na América Latina, podem enfrentar alguns desses desafios. No entanto, como disse um defensor da sociedade civil africana, "reunir-se é uma coisa e fazer mudanças, de fato, é outra". Embora os reguladores da APD se reúnam e troquem as melhores práticas, implementá-las depende de recursos, força de vontade e outros fatores que podem prejudicar a fiscalização regional mais coesa.

Por fim, a participação em fóruns internacionais para colaboração regulatória inevitavelmente pode refletir desigualdades globais históricas. Por exemplo, um regulador africano refletiu sobre experiências recentes com redes regulatórias globais sobre privacidade e acesso à informação:

> Quando olho para a Global Privacy Network, acho que as vozes dos países africanos são um pouco abafadas, não intencionalmente, mas em todos os lugares. [...] A Conferência Geral Anual da ICIC [Conferência Internacional de Comissários de Acesso à Informação], sobre acesso [às informações públicas] de acesso, vai ser realizada no México. Eu dei uma olhada no programa. Não tem a participação de nenhum africano. Daí eu tenho que dizer, mas como é que não há nenhum africano no programa? [...] Você tem que lutar por espaço o tempo todo. Caso contrário, seremos esquecidos.

Assim, embora as APDs do Sul Global possam se beneficiar bastante da participação em redes regionais, elas podem sofrer marginalização em fóruns internacionais.

### Colaboração com agências reguladoras nacionais

As APDs também colaboram com reguladores de agências reguladoras locais, como aquelas que supervisionam a política de concorrência, proteção ao consumidor e regulamentação financeira. À medida que a digitalização se expande, a regulamentação de dados se cruza com um número cada vez maior de domínios de políticas, e a colaboração entre vários reguladores é cada vez mais necessária. Como um regulador africano descreveu,

> Colaboramos com instituições que possam ter um mandato sobreposto, por assim dizer, ou áreas semelhantes como a Comissão da Concorrência, por exemplo, como a Comissão Nacional do Consumidor. Assinamos memorandos de entendimento. Não apenas isso. Também colaboramos com a Comissão

> Eleitoral que administra as eleições. [...] Eles têm que tratar dados em suas listas de eleitores, sabe. Portanto, temos colaboração com organizações semelhantes que são de natureza regulatória.

No entanto, essa colaboração é desigual. Por exemplo, representantes da sociedade civil latino-americana revelaram que a comunicação inter-regulatória geralmente ocorre de modo informal, e não em um nível administrativo formal que resulta em ações vinculantes e está aberta ao escrutínio público. Além disso, as novas APDs podem ser menos experientes e mais lentas do que outras agências, interrompendo a possível harmonização. Por exemplo, em março de 2021, a APD brasileira investigou a atualização planejada da política de privacidade da Meta, que buscava integrar fluxos de dados entre o serviço de mensagens WhatsApp, usado por mais da metade da população do país,[103] e outros serviços da empresa. Segundo os entrevistados, a APD demorou a analisar o caso, o que, por sua vez, atrasou outros órgãos.

Às vezes, a falta de independência das APDs também pode criar atrito colaborativo; elas podem estar menos dispostas a lidar com investigações no setor público do que outras agências mais independentes, que são mais livres para fazê-lo. Por outro lado, o potencial de colaboração pode ser prejudicado quando a APD deve sancionar outra agência reguladora por práticas de dados não compatíveis. Como um regulador africano relatou:

> Durante a gestão da COVID, o Departamento Nacional de Saúde tornou-se custodiante de muitos dados de pessoas que tiveram resultados de teste positivos [para realizar rastreamento de contatos.] Os regulamentos que adotamos sob a Lei Nacional de Estado de Calamidade afirmam: seis semanas após o fim do estado de calamidade nacional, o Departamento Nacional de Saúde deve excluir essa informação ou desidentificá-la se quiser usá-la para esses fins. E assim que o estado de calamidade nacional chegou ao fim [...] eles voltaram e disseram: "Precisamos de um mês". Eles ainda não fizeram o que pede a lei. Isso significa que eles nos forçarão a usar nossos poderes para obrigá-los a fazer isso.

Consequentemente, embora a colaboração com outras instituições reguladoras nacionais seja cada vez mais essencial, essas próprias agências podem se tornar alvos de ações de cumprimento.

### Colaboração com organizações da sociedade civil

As organizações da sociedade civil servem como parceiros instrumentais das APDs. Como observou um agente da sociedade civil africana, "o maior papel das OSCs

[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.

[organizações da sociedade civil] seria supervisionar e garantir a prestação de contas de qualquer forma que possa ser necessária no estágio em que o país se encontra". Outro se referiu a ambas as partes como "aliados naturais". Por exemplo, entrevistados de APDs africanas listaram campanhas da sociedade civil para aumentar a conscientização pública sobre proteção de dados e treinamentos para vários agentes do setor privado, incluindo saúde, seguros e mídia, como especialmente úteis. Os treinamentos ajudaram especialmente a aumentar a conformidade regulatória. Como um entrevistado apontou, as organizações da sociedade civil têm um alcance público maior do que as APDs em alguns momentos, dando-lhes uma vantagem na elaboração de campanhas eficazes de conscientização. De maneira mais ampla, as organizações da sociedade civil no Sul Global desempenham um papel vital como cães de guarda: um regulador africano observou que um relatório da sociedade civil no país resultou na primeira investigação da APD. Da mesma forma, como relatou um representante da sociedade civil latino-americana, geralmente "depois que treinamos a mídia e fazemos uma denúncia, uma denúncia pública, as autoridades começam a investigar" o ofensor.

Além disso, as organizações da sociedade civil auxiliam nas investigações e no cumprimento. Um entrevistado de uma importante organização da sociedade civil latino-americana argumentou que o principal objetivo da organização é fortalecer e apoiar a APD, aumentando a conscientização sobre a proteção de dados e auxiliando em litígios. Essa assistência pode envolver a apresentação de *amici curiae* aos tribunais e o fornecimento de argumentos jurídicos e técnicos às APDs para ganhar casos de proteção de dados. Por exemplo, as organizações da sociedade civil desempenharam um papel fundamental ao ajudar a APD brasileira a contestar a atualização da política de privacidade da Meta para o WhatsApp em 2021. Eles não apenas criaram um senso de urgência em torno do caso, chamando a atenção do público para a mudança de privacidade problemática da empresa estrangeira, mas também aconselharam os reguladores em sua investigação.

Apesar da relação aparentemente natural entre a sociedade civil e as APDs, vários fatores podem impedir colaborações efetivas. As organizações da sociedade civil contam com o apoio de doadores e, como as APDs, podem enfrentar restrições de recursos, o que pode prejudicar sua capacidade de aumentar a conscientização pública, monitorar o espaço de proteção de dados e auxiliar nas investigações e nos procedimentos de execução. Além disso, a capacidade das organizações da sociedade civil de se engajar nessas atividades e desenvolver relacionamentos com os reguladores depende da saúde do espaço cívico. Como observou um defensor da sociedade civil africana,

> Se o espaço cívico está fechando [...], ele pode apresentar desafios muito difíceis para o trabalho, como advocacia ou capacitação e tudo mais. E se também há falta de confiança ou a relação entre a sociedade civil e o executivo é muito artificial, às vezes quando você tenta introduzir o executivo, descobre que existe

> essa animosidade. E também enfrentamos o desafio do desinteresse geral do executivo.

Representantes da sociedade civil de vários países africanos e latino-americanos relataram desafios relacionados ao acesso a reguladores e procedimentos regulatórios. Outro desafio, como enfatizou um defensor, é "uma lacuna de habilidades dentro da própria sociedade civil, o que torna o conhecimento [técnico] concentrado em pouquíssimas pessoas", dificultando o recrutamento de especialistas locais. Outros observaram que os objetivos entre a sociedade civil e os reguladores podem divergir. Por exemplo, um defensor da África argumentou que as organizações da sociedade civil tratam da proteção de dados "por meio de uma perspectiva de direitos humanos [enquanto] os governos nunca fazem isso". Por outro lado, um regulador observou que as organizações da sociedade civil às vezes podem ter um foco único (como defender exclusivamente proteções de privacidade mais fortes), enquanto os reguladores geralmente devem equilibrar vários objetivos, como direitos de privacidade e acesso à informação. Além disso, um regulador africano afirmou que a sociedade civil pode não ter uma abordagem "equilibrada" para a defesa da proteção de dados que reconheça que

> muitas de nossas empresas não podem inovar se não utilizarem dados. Sabemos que os dados são úteis em termos de tomada de decisões informadas, de melhor prestação de serviços e afins. Mas a interpretação da sociedade civil é realmente muito extrema: "São meus dados, você não pode utilizá-los." [...] Em muitos casos, nem sequer apreciará o que o governo fez [como aprovar leis]. [...] [Isso] cria muito atrito com o governo, o que acaba afetando a forma como fazemos parte do nosso trabalho.

Encontrar o equilíbrio entre proteger os direitos de dados e, ao mesmo tempo, não sufocar as economias digitais emergentes pode causar atrito entre a sociedade civil e as APDs.

# Melhores Práticas e recomendações para os desafios enfrentados pelas APDs

Os desafios identificados acima muitas vezes se inter-relacionam e se sobrepõem. Por exemplo, a falta de familiaridade do público e a marginalização dos políticos quanto às questões de proteção de dados não apenas frustram os esforços para criar de APDs, mas também para garantir financiamento para eles, recrutar especialistas, garantir a conformidade e cumprir efetivamente as leis de privacidade. Da mesma forma, o cumprimento efetivo requer financiamento suficiente, independência robusta, conscientização significativa dos setores público e privado sobre direitos de privacidade e leis de proteção de dados e um alto grau de conformidade. Consequentemente, os

problemas das APDs estão frequentemente interligados e, portanto, requerem soluções multifacetadas. Ao mesmo tempo, soluções individuais podem resolver mais de um problema. Diversas recomendações e melhores práticas e surgiram das experiências de APDs e agentes da sociedade civil que trabalham na proteção de dados na África e na América Latina discutidas abaixo.

## 1. Defender a independência da APD desde o início reforça a independência no futuro

Como a independência é essencial para uma APD eficaz, os reguladores que buscam criar APDs devem torná-la uma prioridade. Como um participante da mesa redonda enfatizou: "Se você não afirmar sua independência no início, será muito difícil recuperá-la." Vários países oferecem possíveis abordagens estruturais para maximizar a independência da APD. Por exemplo, Maurício e África do Sul têm autonomia jurídica, econômica e administrativa, reportando-se apenas ao Parlamento, enquanto a APD da Argélia é governada por um conselho com representantes de todos os ramos do governo, diluindo sua influência individual.[104] Os entrevistados destacaram a importância de separar os orçamentos da APD do executivo como outro fator essencial. Para as APDs existentes que enfrentam ameaças à independência, a sociedade civil pode desempenhar um papel significativo conduzindo e divulgando pesquisas independentes e relatórios públicos, principalmente no âmbito da comunidade local, para promover uma demanda e uma cultura de independência.[105]

## 2. Garantir que os valores e as necessidades locais sejam equilibrados com a proteção de dados preliminar desde o início é essencial para a legitimidade e eficácia da APD

Embora os marcos europeus de proteção de dados sirvam como padrão-ouro internacional, eles não se traduzem automaticamente em outras regiões, especialmente na ausência de uma infraestrutura legal e regulatória equivalente. A harmonização regulatória pode fornecer benefícios significativos, inclusive no que diz respeito às transferências de dados transnacionais que facilitam a participação nas economias globais de dados. No entanto, a criação e implementação de marcos locais de proteção de dados requer a consideração de culturas e capacidades legais e regulatórias locais, muitas vezes únicas, bem como realidades econômicas. Concretamente, a criação pode envolver uma série de consultas com vários representantes dos setores público e privado. Esse envolvimento público deve ser complementado com pesquisas que analisem como a exploração de dados e os danos decorrentes se desdobram e afetam diferentes contextos e setores locais. Da mesma forma, a implementação de marcos de

[104] Ademuyiwa e Adeniran, "Assessing Digitalization and Data Governance Issues in Africa."
[105] Internet Society, "Personal Data Protection Guidelines for Africa."

proteção de dados pode envolver a implementação de conformidade e aplicação em fases de referência para garantir espaço suficiente para feedback e conformidade dos setores público e privado. Sem esse envolvimento público, o feedback e a avaliação cuidadosa das necessidades e preocupações locais, a legitimidade pública de uma APD pode ser prejudicada. Além disso, próprias populações que correm maior risco de ter seus dados mal utilizados podem não entender as questões de proteção de dados, perpetuando estereótipos sobre as preocupações com a privacidade como domínio de políticos e elites ricas.

## 3. A colaboração com a sociedade civil é essencial para as funções básicas e a legitimidade da APD

Como vários participantes da mesa redonda enfatizaram, apesar dos objetivos às vezes divergentes, a colaboração com a sociedade civil é essencial para cultivar a conscientização local sobre os direitos e as obrigações de privacidade. Como observou um regulador, "observamos muita atividade na sociedade civil. Acho que isso é uma oportunidade, pois eles são capazes de levar nossa voz a locais onde não estamos. ... [Nós] colaboramos muito com eles, principalmente na conscientização sobre a denúncia de organizações que não estão em conformidade." Eles continuam sendo parceiros cruciais na educação do público, o que pode aumentar a legitimidade das APDs, mas também na conscientização do setor privado. Particularmente, nomear e envergonhar os infratores podem ajudar no cumprimento e na melhoria da conformidade. Por exemplo, na América Latina, as ONGs preencheram uma lacuna importante de cumprimento ao defender a transparência nas solicitações de dados governamentais de provedores de serviços de Internet; uma tarefa que está fora do mandato de muitas APDs regionais devido a isenções legais para entidades públicas.[106]

## 4. A colaboração entre as APDs pode reunir recursos, aumentar a conscientização e fortalecer o cumprimento

Apesar de certos desafios associados à colaboração entre APDs, o consenso esmagador entre os reguladores de dados é que a prática é imensamente benéfica para aumentar a conscientização, fortalecer o cumprimento e compartilhar as melhores práticas. Como disse um participante da mesa redonda, "a cooperação internacional [e] o desenvolvimento da cooperação entre os membros da rede [podem] melhorar a visibilidade no cenário mundial, criar uma rede de compartilhamento com os órgãos da África, desenvolver ferramentas e capacitar o desenvolvimento dos membros". Outro regulador visitou APDs na Europa e na América do Norte para conhecer as melhores práticas como uma das etapas preliminares para o lançamento de uma comissão africana. Também há oportunidade de colaboração entre regiões do Sul Global, mas

[106] Rodriguez e Alimonti, "A Look-Back and Ahead on Data Protection in Latin America and Spain."

embora pelo menos um marco de proteção de dados africano tenha se inspirado em um de origem latino-americana, os entrevistados não estavam cientes de nenhuma colaboração explícita.

Essa colaboração e consulta não precisam sobrecarregar os objetivos, os valores ou as necessidades locais, especialmente porque existem muitas diferenças culturais, econômicas e outras importantes tanto dentro das regiões quanto entre países individuais.[107] Em vez disso, como as APDs na África e na América Latina geralmente enfrentam problemas semelhantes (como restrições de financiamento, conscientização limitada), a colaboração pode priorizar a abordagem de questões comuns. Além disso, a aplicação coordenada pode aumentar a probabilidade de sancionar com sucesso o descumprimento de big techs.[108] Por fim, embora a harmonização permaneça indefinida, os esforços para harmonizar os marcos podem fornecer previsibilidade crucial para empresas que operam internacionalmente e, com isso, aumentar a conformidade geral.

## 5. O direcionamento e o enquadramento estratégicos de mensagens e a criação de relacionamentos entre as APDs e a mídia podem ajudar a aumentar a conscientização

Alguns esforços para aumentar a conscientização são especialmente eficazes. Uma abordagem concreta para comunicar ao público os riscos das violações de privacidade é vincular as preocupações com a proteção de dados a danos concretos na vida real.[109] Como o desejo de participar das economias de dados globais serve como um forte incentivo para desenvolver leis de proteção de dados e reforçar o cumprimento,[110] enfatizar os benefícios econômicos de uma sólida regulamentação e conformidade de dados pode repercutir tanto no setor privado quanto nos formuladores de políticas. Esse enquadramento pode aumentar o apoio dos formuladores de políticas às APDs e possivelmente ajudar a retardar a conformidade, vinculando boas práticas de dados do setor privado ao sucesso econômico. Nesse sentido, um regulador africano enfatizou a utilidade das ferramentas digitais para alcançar a classe trabalhadora experiente em tecnologia e aumentar a conscientização sobre os direitos e as responsabilidades de proteção de dados: “Temos webinars mensais nos quais discutimos assuntos atuais, e nossa participação tem sido boa [...] E isso nos custou muito pouco. [...] Sem colocar publicidade, conseguimos chegar muito longe.” Outra oportunidade para aumentar a conscientização, como argumentou o ex-regulador, é desenvolver relacionamentos mais sólidos entre as APDs e a mídia. Esses relacionamentos podem não apenas aumentar a conscientização do público sobre questões de proteção de dados –

[107] por exemplo, Sutherland, “The Governance of Data Protection in South Africa.”
[108] Davis, “Data Protection in Africa: A Look at OGP Member Progress.”
[109] Ibid.
[110] Bryant, “Africa in the Information Age.”

melhorando potencialmente a conformidade e o cumprimento – mas também aumentar a transparência em torno dos procedimentos da APD.

## 6. A colaboração com outras agências reguladoras, a adoção de uma abordagem baseada em risco e o fortalecimento do sistema judicial podem reforçar o cumprimento

Para enfrentar os desafios de fiscalização, que muitas vezes são exacerbados por recursos e capacidade limitados, os especialistas defendem soluções criativas. Por exemplo, Suyash Rai, da Carnegie India, argumenta que, como a "capacidade de uma APD será limitada no início de seu mandato, a instituição deve usar uma abordagem baseada em risco com o objetivo de direcionar recursos para áreas nas quais os riscos são maiores, a fim de evitar sobrecarga.[111] Além disso, o uso de RegTech (tecnologia regulatória) para automatizar o processamento de reclamações pode ajudar a enfrentar os desafios de capacidade. Da mesma forma, priorizar os recursos existentes para criar um registro público de infratores como sanção à reputação também pode aumentar a conformidade e reduzir os encargos de cumprimento.[112] Um entrevistado também enfatizou que a colaboração com outras agências reguladoras de um país pode melhorar o cumprimento e a conformidade. O entrevistado, um regulador na África, observou melhores taxas de conformidade nos setores financeiro, de seguros e de telecomunicações, argumentando que "trabalhar com reguladores realmente ajudou e é algo que queremos continuar e garantir que possamos integrar mais pessoas". Geralmente, as APDs que têm mandatos transversais estão bem posicionadas para envolver várias partes interessadas, incluindo a sociedade civil e outros reguladores.[113] Dado que vários entrevistados relataram desafios relacionados à inexperiência judicial no julgamento de casos de proteção de dados, o fortalecimento e a capacitação técnica dos tribunais também é um fator essencial para um cumprimento mais eficaz.[114]

## 7. Financiamento de programas de educação para cultivar a experiência local e a conscientização do público

Como indica a liderança da África do Sul em proteção de dados na África, advogar pela inclusão de questões de dados e privacidade como parte dos currículos universitários pode aumentar a experiência local e a alfabetização digital.[115] Da mesma forma, um ex-regulador latino-americano enfatizou a importância de cultivar o conhecimento local por meio da educação. Tal esforço exigiria não apenas a expansão dos currículos nas faculdades de direito e nos departamentos de ciência da computação, mas também a

[111] Pisa e Nwankwo, "Are Current Models of Data Protection Fit for Purpose?," 4.
[112] Pisa e Nwankwo, "Are Current Models of Data Protection Fit for Purpose?"
[113] Ademuyiwa e Adeniran, "Assessing Digitalization and Data Governance Issues in Africa."
[114] ver também Abdulrauf e Fombad, "Personal Data Protection in Nigeria."
[115] Makulilo, "Privacy and Data Protection in Africa."

alfabetização digital nas universidades. O financiamento de cursos acadêmicos que envolvem proteção de dados e fluxos de dados pode criar um canal para futuras autoridades, bem como cultivar a conscientização pública e o diálogo sobre questões de proteção de dados.

## 8. O apoio às redes nacionais e regionais da sociedade civil pode reforçar as investigações de cumprimento

Entrevistados da sociedade civil enfatizaram que a criação de redes regionais entre organizações da sociedade civil nos países e entre eles pode estimular as investigações de cumprimento. Essas redes podem resultar em ajuda mútua, principalmente em grandes casos legais. Um entrevistado os descreveu como "efeitos de rede": com um número substancial de colaborações das organizações, os defensores tornaram-se mais eficazes na obtenção de documentos regulatórios, na elaboração de documentos jurídicos especializados e em outras funções de apoio. Além disso, essas redes colaborativas serviram como uma fonte crucial de apoio social e motivação para os litigantes civis envolvidos em processos desafiadores e que demandam tempo e recursos, como o caso WhatsApp no Brasil.

## 9. O desenvolvimento de espaços cívicos abertos e a criação de redes locais de agentes políticos pode proteger e reforçar a independência e a responsabilidade da APD

Embora as APDs implementem e apliquem marcos de proteção de dados, a proteção de dados é, em última análise, um esforço colaborativo que requer redes sólidas e espaços cívicos saudáveis. A sociedade civil pode ajudar a cultivar oportunidades e espaços cívicos para criar essas redes, nas quais vários agentes políticos possam se envolver em discussões abertas sobre questões de proteção de dados. Um representante da sociedade civil latino-americana deu um exemplo dessas reuniões que ocorreram em seu país:

> [Acho importante] organizar seminários técnicos nos quais as pessoas possam falar livremente o que pensam sobre qual deve ser a melhor abordagem regulatória para proteção de dados. [...] Nos últimos dez anos, organizamos [esses] seminários. [...] As pessoas se sentiram em um espaço seguro, [...] pessoas do governo, promotores federais, advogados [...] sociedade civil, ativistas e assim por diante. [...] Foi um espaço para diálogos, para aprofundar algumas questões políticas e até para discordar no final. Mas acho que isso foi muito importante para criar confiança. [...] Acredito que isso também foi fundamental para criar relações com os membros da APD.

A criação de estruturas que cultivem espaços cívicos robustos de livre intercâmbio é essencial para a criação de redes duráveis de agentes políticos investidos no

desenvolvimento de marcos sólidos de proteção de dados e na supervisão. Mesmo quando o espaço cívico nacional é reduzido ou fechado, essas reuniões podem servir como blocos de criação de redes de responsabilidade mútua que fornecem verificações cruciais sobre ameaças à independência regulatória.

# Sobre os autores

**Pawel (Paul) Popiel** é bolsista de Pós-Doutoramento George Gerbner na Annenberg School for Communication, Universidade da Pensilvânia. Sua pesquisa, que examina como a política molda a governança da mídia digital e das tecnologias emergentes, foi publicada em revistas como *Policy & Internet*, *Critical Studies in Media Communication*, *Journal of Digital Media & Policy*, *Journal of Broadcasting & Electronic Media* e outras, e foi apresentada em grandes conferências. Possui doutorado pela Annenberg School for Communication, Universidade da Pensilvânia. Ele também é bacharel em Ciência Política pela Universidade McGill e mestre em Estudos de Mídia pela Universidade do Texas em Austin.

**Laura Schwartz-Henderson** é a Assessora de Pesquisa e *Advocacy* da equipe de Tecnologia Global da Internews, onde desenvolve ferramentas estratégicas de *advocacy*, programas e pesquisa sobre política tecnológica, ecossistemas de mídia e movimentos sociais. Anteriormente, Laura foi Pesquisadora e Gerente de Políticas do curso de Democracia Digital do German Marshall Fund e Gerente de Projetos de Pesquisa no Observatório de Políticas da Internet na Annenberg School for Communications da Universidade da Pensilvânia. Ela tem uma vasta experiência na condução de pesquisas sobre questões de direitos digitais, gestão de programas e trabalho com ativistas e jornalistas em diversos contextos políticos. Possui mestrado em Administração Pública pela Universidade da Pensilvânia. Sua pesquisa se concentra nos mecanismos pelos quais a tecnologia atua como mediadora no envolvimento cívico e as arquiteturas e culturas institucionais de justiça social e organizações filantrópicas. É fundadora da Creative Digital Rights Advocacy Collab Network e a produtora executiva do podcast Privacy is Global.

O **Professor Eduardo Bertoni** (Doutorado, Universidade de Buenos Aires) é atualmente o Representante do Escritório Regional para a América do Sul do Instituto Interamericano de Direitos Humanos. Foi o primeiro Diretor da Agência de Acesso à Informação Pública (AAIP) que é a Autoridade Argentina de Proteção de Dados e Acesso à Informação. Foi o fundador e o primeiro diretor do Centro de Estudos sobre Liberdade de Expressão e Acesso à Informação (CELE) da Faculdade de Direito da Universidade de Palermo, Argentina. Foi Diretor Executivo da Due Process of Law Foundation (DPLF) até maio de 2006. Anteriormente, foi Relator Especial para a Liberdade de Expressão da Comissão Interamericana de Direitos Humanos da Organização dos Estados Americanos (2002–2005).