COORDENAÇÃO
ALESSANDRA BORELLI
RENATO OPICE BLUM

ORGANIZAÇÃO
JAYME DOMINGUES

PRIVACIDADE E DIREITO DIGITAL

ÉTICA, INOVAÇÃO E O FUTURO DOS NEGÓCIOS

2027

EDITORA JusPODIVM
www.editorajuspodivm.com.br

PARTE 11

GOVERNANÇA DIGITAL E RESPONSABILIDADE CORPORATIVA

DESAFIOS DA CONFORMIDADE REGULATÓRIA PARA DIFERENTES PERFIS DE EMPRESAS

Manuella Filadoro[1]
Ana Filadoro[2]

INTRODUÇÃO

Quando ouvimos falar de conformidade regulatória, a primeira coisa que pensamos está diretamente relacionada a organizações que atuam em setores regulados.

Por muitos anos, foi difícil pensar em organizações fora do setor regulatório que precisassem estar de acordo com alguma regulação não emitida em formato legislativo.

Esse assunto pode parecer novo no Brasil, mas não é considerado novo ao redor do mundo, isso porque, no mundo atual, a conformidade é considerada um fator essencial de um modelo de gestão empresarial inovador e

1. Advogada Sênior do Opice Blum Advogados; Mestre em Direito Digital pela Universidade Presbiteriana Mackenzie; especialista em Direito Empresarial e Contratual pelo INSPER; Professora da Opice Blum Academy; da Escola Paulista de Direito e da Galícia Educação. Possui as certificações de DPO da Universidade de Maastrich, CIPP/e, CIPM e CDPO/BR da International Association of Privacy Professionals (IAPP) e EXIN Essentials.

2. General Counsel atuante entre Europa e América Latina com foco em regulação, expansão e mitigação de riscos jurídicos; Mestre em Direito Tributário e Societário pelo INSPER; MBA Executivo pela London School of Economics. Foi DPO de grupos internacionais de tecnologia, com atuação em SaaS, cripto e fintech em 14 jurisdições. Certificada como DPO pela Universidade de Maastricht e em Negociação Executiva pela Harvard Law School. Premiada como Woman in Law – Rising Star 2024 pela World Law Alliance.

consciente, especialmente diante da crescente criação de novas normas regulatórias e de suas complexidades em âmbitos nacionais e internacionais.

No contexto europeu, questões relacionadas à conformidade surgiram muito antes do famigerado Regulamento Geral sobre Proteção de Dados (GDPR), normativo que deu início a uma corrida mundial para estabelecimento de leis que objetivavam proteger a privacidade dos indivíduos.

Na Europa, já se pensava em privacidade e proteção de dados há muitos anos, mas o marco específico sobre o tema veio com a Convenção 108, acordada em 1981.

No contexto brasileiro, somente começamos a falar sobre proteção de dados com mais veemência após o surgimento do Regulamento Geral sobre a Proteção de Dados (GDPR), uma vez que esse foi responsável por impor novos padrões de responsabilidades e transparência para organizações que tratam dados pessoais não só dentro na União Europeia, como em países que possuem alguma relação comercial com a Europa.

É nítido que a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) foi inspirada no regulamento europeu, e trouxe um protagonismo quando falamos em conformidade regulatória em privacidade e proteção de dados, que passou a desempenhar um papel central na estratégia de conformidade de organizações.

Esse cenário se intensifica com o rápido surgimento de tecnologias baseadas em inteligência artificial (IA), que resultam em uma nova forma de responsabilização e controle. A utilização de sistemas automatizados para tomada de decisões, coleta e análise de dados em larga escala levanta muitas questões sobre transparência, explicabilidade e discriminação algorítmica. Ainda que a regulamentação de IA esteja em estágios iniciais no Brasil, há uma tendência global de integração entre os marcos legais de proteção de dados e os regimes de controle de tecnologias emergentes.

Diante desse contexto, o presente artigo analisa os desafios da conformidade regulatória em proteção de dados e privacidade enfrentados por empresas com diferentes perfis, considerando suas especificidades estruturais, operacionais e de governança. A abordagem será segmentada em *startups*, Microempresas e Empresas de Pequeno Porte, grandes empresas nacionais e grupos multinacionais. Também serão exploradas as boas práticas de adequação, de forma proporcional à complexidade e aos riscos próprios de cada perfil, com referências à regulação de inteligência artificial como tema emergente relevante.

O objetivo é oferecer uma visão comparativa e orientada à prática sobre como diferentes tipos de organizações podem (e devem) estruturar seus programas de conformidade em um cenário regulatório em constante evolução, marcado pela interseção entre direitos fundamentais, inovação tecnológica e responsabilização corporativa.

1. CONCEITO DE CONFORMIDADE REGULATÓRIA

A conformidade regulatória é considerada como o conjunto de práticas e mecanismos internos adotados pelas organizações com o objetivo de assegurar que as normas legais e regulatórias aplicáveis às suas atividades sejam devidamente observadas e cumpridas. No contexto da sociedade da informação, o conceito passou a englobar, de forma cada vez mais expressiva, obrigações relacionadas à governança de dados, segurança da informação, direitos dos titulares e, mais recentemente, à ética no uso de tecnologias emergentes, como a inteligência artificial.

Na área de proteção de dados pessoais, a conformidade regulatória envolve, entre outros aspectos, a transparência sobre o tratamento dos dados aos titulares, identificação de bases legais para o tratamento de dados, a implementação de medidas técnicas e administrativas de segurança, a garantia dos direitos dos titulares e a responsabilização e prestação de contas (*accountability*). Tais obrigações decorrem da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018[3]), que se insere em um movimento global de reconhecimento do direito à privacidade como direito fundamental e da proteção de dados como valor essencial nas democracias contemporâneas.

No Brasil, inclusive, tivemos a Emenda Constitucional nº 115/2022[4] que incluiu proteção de dados pessoais como direito fundamental, descrito no artigo 5º, inciso LXXIX:

> *LXXIX – é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.*

3. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965/2014 (Marco Civil da *Internet*). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

4. BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 21 maio 2025.

Com a entrada em vigor da LGPD e a criação da Autoridade Nacional de Proteção de Dados (ANPD[5]), a conformidade passou a exigir das organizações uma postura ativa, voltada não apenas ao cumprimento formal da norma, mas também à estruturação de programas robustos de governança em privacidade. Tais programas devem ser compatíveis com a natureza e o porte da organização, o volume e a sensibilidade dos dados tratados e os riscos envolvidos para os titulares, competindo à ANPD, conforme artigo 55-J, inciso XVIII, a edição de normas específicas para Microempresas e Empresas de Pequeno Porte e aquelas que se autodeclaram *startups*[6].

A tendência de regulação setorial e multidisciplinar de tecnologias digitais também vem sendo observada no campo da inteligência artificial. No Brasil, embora ainda não haja um marco regulatório específico em vigor, diversas propostas legislativas estão em debate, e a ANPD já se manifestou no sentido de incluir os sistemas de IA como objeto de atenção no contexto da proteção de dados[7]. Além disso, normas internacionais, como o *AI Act* da União Europeia, indicam um futuro próximo em que o uso de IA estará submetido a exigências regulatórias específicas, inclusive quanto à transparência, explicabilidade e mitigação de riscos discriminatórios[8].

Nesse cenário, a conformidade regulatória deixa de ser apenas uma exigência legal e passa a se configurar como elemento estratégico, capaz de agregar valor à organização, gerar confiança aos usuários e parceiros, e mitigar riscos jurídicos, reputacionais e financeiros. Entretanto, os meios para

5. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Guia de boas práticas: programa de governança em privacidade. Versão 2.3. novembro 2024. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_programa_governanca_privacidade.pdf. Acesso em: 26 maio 2025..

6. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais – LGPD. Art. 55-J, XVIII: editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 21 maio 2025.

7. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Relatório Preliminar sobre Regulação de Inteligência Artificial e Proteção de Dados Pessoais. 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/analise-preliminar-do-pl-2338_2023-formatado-ascom.pdf . Acesso em: 26 maio 2025.

8. UNIÃO EUROPEIA. Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho (AI Act). Brussels, 2024. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=OJ:L_202401689. Acesso em: 26 de maio de 2025.

atingir esse objetivo variam significativamente de acordo com o perfil da empresa, suas capacidades internas e sua exposição aos riscos regulatórios.

2. PANORAMA REGULATÓRIO BRASILEIRO EM PROTEÇÃO DE DADOS E TECNOLOGIAS EMERGENTES

O cenário regulatório brasileiro relacionado à proteção de dados pessoais passou por uma transformação significativa a partir da promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD), que estabeleceu um marco normativo principiológico, aplicável a praticamente todos os setores da economia. Conforme já mencionado anteriormente, a LGPD, inspirada no Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR), introduziu uma nova lógica regulatória baseada em responsabilidade proativa, transparência e foco no risco.

No entanto, diferentemente do que ocorreu na União Europeia, em que a privacidade e a proteção de dados já eram assuntos pautados como importantes há muitos anos, no Brasil, sua importância somente foi aventada quando da publicação do Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR), que estabeleceu uma série de exigências e padrões específicos de privacidade até então desconhecidos no Brasil.

A promulgação da LGPD e a criação da Autoridade Nacional de Proteção de Dados (ANPD), com poderes normativos e sancionatórios, consolidaram um novo patamar de exigência regulatória, exigindo das organizações a estruturação de políticas internas voltadas ao tratamento de dados, processos de mapeamento, relatórios de impacto, mecanismos de resposta a incidentes de segurança e canais de atendimento aos titulares. A conformidade passou a ser monitorada não apenas por meio da aplicação da lei, mas também a partir da atuação da ANPD na edição de guias, resoluções, regulamentos e notas técnicas, como o Regulamento de Dosimetria de Sanções[9] e a Regulamentação do tratamento de dados pessoais pelo agente de pequeno porte[10].

9. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria/Resolucaon-4CDANPD24.02.2023.pdf. Acesso em: 26 maio 2025.

10. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Regulamentação do tratamento de dados pessoais pelo agente de pequeno porte. Resolução CD/ANPD nº 2, de 27 de janeiro de 2022. Disponível

Além disso, a proteção de dados tornou-se questão multissetorial em diversas esferas regulatórias, sendo incorporada em normativos da Agência Nacional de Saúde Suplementar (ANS[11]), Banco Central do Brasil (Bacen), Comissão de Valores Mobiliários (CVM[12]), entre outros. Essa multiplicidade de fontes normativas reforça a complexidade do cenário para organizações que operam em setores regulados ou que tratam grandes volumes de dados pessoais sensíveis ou financeiros.

Paralelamente ao assunto de proteção de dados, o Brasil tem avançado, ainda que de forma incipiente, na discussão sobre a regulação da inteligência artificial. Em 2023, o Senado Federal apresentou o Projeto de Lei nº 2338[13], inspirado no modelo europeu, como aconteceu com proteção de dados, com foco na classificação de riscos e obrigações proporcionais. O texto propõe diretrizes como a promoção da inovação responsável, o respeito aos direitos fundamentais, a avaliação de impactos algorítmicos e a governança dos sistemas de IA. Embora ainda não convertido em lei, o projeto sinaliza a intenção do legislador brasileiro de antecipar-se aos riscos associados a tecnologias automatizadas e prever uma arquitetura regulatória harmônica com os marcos já existentes, como a LGPD e o Marco Civil da *Internet*.

Por fim, vale destacar que a conformidade regulatória no Brasil se dá em um contexto de assimetria institucional, onde lacunas normativas convivem com interpretações divergentes e, por vezes, sobreposições de competências entre órgãos reguladores. Isso impõe às organizações o desafio de monitorar continuamente a produção normativa, dialogar com múltiplas autoridades e adaptar-se de maneira ágil e efetiva às novas exigências

em https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022. Acesso em: 26 maio 2025.

11. AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR (ANS). ANS e ANPD firmam acordo para aprimorar proteção de dados na área de saúde suplementar. 24 ago. 2023. Disponível em: https://www.gov.br/ans/pt-br/assuntos/noticias/sobre-ans/ans-e-anpd-firmam-acordo-para-aprimorar-protecao-de-dados-na-area-de-saude-suplementar. Acesso em: 21 maio 2025.

12. COMISSÃO DE VALORES MOBILIÁRIOS (CVM). LGPD – Lei Geral de Proteção de Dados Pessoais. Página institucional sobre a LGPD e sua aplicação no âmbito da CVM. Disponível em: https://www.gov.br/cvm/pt-br/assuntos/lgpd. Acesso em: 21 maio 2025.

13. BRASIL. Senado Federal. Projeto de Lei nº 2.338, de 2023. Dispõe sobre o uso da Inteligência Artificial. Autor: Senador Rodrigo Pacheco (PSD/MG). Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Acesso em: 27 maio 2025.

legais e técnicas – especialmente em temas relacionados ao direito digital, que evoluem com velocidade, como privacidade digital e inteligência artificial.

3. DESAFIOS GERAIS PARA A CONFORMIDADE EM PRIVACIDADE E TECNOLOGIAS DIGITAIS

A conformidade em privacidade e proteção de dados pessoais apresenta uma série de desafios que impactam organizações de todos os portes e setores. Embora os obstáculos possam se manifestar de forma distinta conforme o perfil, tamanho e área de atuação da organização, há uma base comum de dificuldades relacionadas à própria natureza das normas de proteção de dados, à dinamicidade tecnológica e à crescente interconexão entre regulação, inovação e competitividade.

3.1. Complexidade e Abstração Normativa

Temos muitas normas brasileiras que acabam por tipificar condutas específicas que podem gerar algum tipo de penalidade à determinado infrator.

A LGPD, à semelhança do GDPR, adotou um modelo principiológico, ou seja, muitas de suas disposições são abertas, exigindo interpretação com base no contexto experimentado e aplicação proporcional ao risco.

Em que pese a estrutura normativa da LGPD garantir flexibilidade e diminuir a necessidade de revisão de condutas ao longo do tempo, é necessário pontuar que o modelo também gera insegurança jurídica, sobretudo em organizações que não dispõem de equipes jurídicas especializadas. Conceitos como "interesse legítimo", "dados pessoais sensíveis", "controlador", "pseudonimização" e "minimização" exigem análise técnica e jurídica constante, muitas vezes sem precedentes consolidados na jurisprudência ou diretrizes suficientemente detalhadas da ANPD[14].

14. BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. São Paulo: Revista dos Tribunais, 2019.

3.2. Evolução Tecnológica Acelerada

A elaboração de normas reguladoras e as novas tecnologias crescem de forma inversamente proporcional, de modo que a velocidade com que novas tecnologias são desenvolvidas e incorporadas aos modelos de negócio impõe desafios significativos aos reguladores e, consequentemente, à conformidade regulatória.

O fato é que sempre teremos um *gap* entre a criação de um novo modelo tecnológico e sua respectiva regulação, mesmo porque ferramentas baseadas em *big data*, biometria, inferência comportamental e, especialmente, inteligência artificial, ampliam a complexidade da análise de riscos e da criação de medidas adequadas de mitigação.

3.3. Cultura Organizacional e Maturidade em Governança

Outro obstáculo recorrente diz respeito à cultura organizacional, que muito se relaciona com a cultura de determinado país. No Brasil, não tínhamos uma cultura de privacidade e proteção de dados até o surgimento da LGPD, de modo que não temos uma cultura forte sobre o assunto na Sociedade, o que reflete na cultura das organizações estabelecidas no país.

Em muitas organizações, sobretudo nas de menor porte, a proteção de dados é ainda percebida como uma exigência burocrática e cara, sem o reconhecimento de seu valor estratégico. A ausência de apoio da alta gestão ("Tone at the Top"), a resistência das áreas estratégicas e a carência de processos estruturados reduzem a efetividade de programas de conformidade.

Essa fragilidade cultural, muitas vezes, está ligada à ausência de incentivos internos e à dificuldade de integrar boas práticas de privacidade à rotina operacional. Tais lacunas comprometem a sustentabilidade das medidas adotadas ao longo do tempo, tendo muitas empresas que possuem um Programa de Privacidade somente no papel e que não é posto em prática.

Além da cultura interna, é fundamental considerar o ambiente regulatório em que as organizações operam – que, como veremos a seguir, impõe seus próprios desafios.

3.4. Multiplicidade de Fontes Normativas

A coexistência de normas gerais e setoriais, emitidas por diferentes órgãos reguladores, representa um desafio contínuo. Empresas que atuam em setores regulados, como os de saúde e financeiro, precisam atender simultaneamente à LGPD e a normativos específicos do Banco Central, da ANS, da ANPD, entre outros.

Essa sobreposição de exigências obriga as organizações a manterem estruturas atualizadas de monitoramento normativo, harmonização de políticas internas e definição de prioridades regulatórias – o que pode ser especialmente complexo para estruturas enxutas ou descentralizadas.

3.5. Necessidade de Capacitação Técnica e Jurídica

A conformidade regulatória requer conhecimento técnico-jurídico multidisciplinar, o que demanda investimento na formação e atualização constante das equipes. Dada a natureza multidisciplinar da proteção de dados, os profissionais envolvidos precisam compreender tanto os fundamentos jurídicos da legislação quanto os aspectos técnicos de segurança da informação, arquitetura de dados, ciclo de vida dos sistemas e lógica algorítmica. A escassez de profissionais capacitados – sobretudo fora dos grandes centros urbanos – agrava esse desafio e limita a capacidade de resposta das empresas às exigências regulatórias.

4. DESAFIOS POR PERFIL DE EMPRESA: ANÁLISE COMPARATIVA

A implementação de programas de conformidade em privacidade e proteção de dados pessoais não é uniforme e deve ser adaptada às características específicas de cada organização, como reforçado diversas vezes pelo legislador ao longo do texto da LGPD.

Elementos como porte, maturidade, internacionalização, complexidade da operação, apetite de risco da organização e grau de exposição a riscos regulatórios moldam a forma como os desafios se apresentam e devem ser enfrentados. A seguir, são analisados comparativamente os principais obstáculos enfrentados por quatro perfis típicos de empresas: *startups*,

microempresas e empresas de pequeno porte, grandes empresas nacionais e grupos multinacionais.

4.1. *Startups*

Startups operam sob condições de elevada incerteza, mudanças constantes, ciclos rápidos de iteração e foco na escalabilidade. Nesse contexto, a conformidade regulatória tende a ser percebida como um custo não prioritário – especialmente em fases iniciais de desenvolvimento do produto. O risco, porém, é significativo: soluções tecnológicas escaláveis frequentemente envolvem o tratamento massivo de dados pessoais (plataformas de saúde, *fintechs, marketplaces* etc.), muitas vezes sem a devida análise legal prévia.

Além disso, a ausência de estruturas jurídicas internas e a dependência de investidores externos podem dificultar a implantação de medidas adequadas de governança em privacidade. Muitos modelos de negócio baseiam-se na coleta de dados comportamentais, uso de algoritmos e segmentação automatizada, o que exige avaliações de impacto e documentação mínima, sob risco de futuras sanções ou perda de confiança dos usuários. Há, contudo, oportunidades: a adoção de *privacy by design* e *security by design* desde o início do desenvolvimento pode ser uma vantagem competitiva e um fator de atração de investimentos.

4.2. Microempresas e Empresas de Pequeno Porte

As microempresas e empresas de pequeno porte[15] enfrentam o desafio da escassez de recursos financeiros, humanos e tecnológicos. Embora sujeitas às mesmas obrigações legais das grandes corporações, muitas vezes não dispõem de equipes dedicadas à proteção de dados, tampouco de capacidade financeira para fazer frente aos custos de contratação de consultorias externas especializadas. A própria ANPD reconhece essa limitação, tendo editado norma específica para agentes de tratamento de pequeno

15. BRASIL. Lei Complementar nº 123, de 14 de dezembro de 2006. Institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp123.htm. Acesso em: 27 maio 2025.

porte, com flexibilizações proporcionais ao risco do tratamento de dados realizado[16].

Apesar disso, muitas microempresas e empresas de pequeno porte atuam como operadores de dados pessoais para empresas maiores, ou seja, em seu nome e sob suas instruções, de modo que são cobradas por seus parceiros comerciais quanto ao cumprimento da LGPD – especialmente em setores regulados.

A conformidade, assim, deixa de ser apenas uma obrigação legal e passa a ser um requisito de mercado. Entre os principais gargalos estão a falta de registros de tratamento, ausência de políticas internas mínimas e carência de treinamentos sobre privacidade e segurança da informação.

4.3. Grandes Empresas Nacionais

Organizações de médio e grande porte já estruturadas tendem a possuir departamentos jurídicos, de *compliance* e de tecnologia que permitem a implementação de programas mais robustos de governança em privacidade. Os desafios, contudo, são proporcionais à complexidade de sua operação. Muitas dessas empresas acumulam legados de sistemas com baixa integração, dificultando a rastreabilidade e a aplicação de princípios como a minimização e a limitação de finalidade.

Além disso, a descentralização das decisões, a existência de múltiplas unidades de negócio e a resistência cultural em setores tradicionais podem comprometer a efetividade das medidas adotadas. A estruturação de um programa de conformidade requer diagnóstico aprofundado, envolvimento da alta gestão (*Tone at the Top*), priorização de riscos e investimentos. A responsabilidade pelo tratamento de grandes volumes de dados – incluindo dados pessoais sensíveis – aumenta a exposição a sanções, ações coletivas e danos reputacionais, exigindo respostas organizacionais mais maduras.

16. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Regulamentação do tratamento de dados pessoais pelo agente de pequeno porte. Resolução CD/ANPD nº 2, de 27 de janeiro de 2022. Disponível em https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022. Acesso em: 26 maio 2025.

4.4. Grupos Multinacionais

Empresas multinacionais enfrentam o desafio adicional de harmonizar exigências regulatórias de diferentes jurisdições, uma vez que é comum que estejam sujeitas a diferentes legislações pelo mundo de forma simultânea, como à LGPD, ao GDPR, à CCPA (Califórnia) e a outras legislações de proteção de dados.

Como cada uma das legislações pelo mundo possuem exigências específicas quanto à transferência internacional de dados, contratação de encarregados pelo tratamento de dados (*Data Protection Officer* ou DPO), notificações de incidentes e direitos dos titulares, os Grupos Multinacionais enfrentam um grande desafio para sua conformidade regulatória. A adoção de normas corporativas globais (*Binding Corporate Rules*) é um instrumento recorrente e aliado aos Grupos Multinacionais no momento do compartilhamento de informações entre empresas do grupo, mas, ao mesmo tempo, demanda esforço jurídico e organizacional considerável, além de necessitar da chancela da ANPD para ser posta em prática no Brasil[17]

Além disso, essas organizações frequentemente utilizam sistemas baseados em inteligência artificial para análise de dados em escala global, o que adiciona camadas de complexidade à avaliação de riscos, à explicabilidade de decisões automatizadas e à prevenção de impactos discriminatórios. A necessidade de reportar a diferentes autoridades de proteção de dados e de garantir consistência interna nas políticas adotadas demanda governança sólida, coordenação internacional e investimento contínuo em compliance tecnológico.

4.5. Tabela Comparativa: Desafios por Perfil de Empresa

A seguir, apresenta-se uma síntese dos principais desafios enfrentados por diferentes perfis de empresas no contexto da conformidade regulatória:

17. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Regulamento de Transferência Internacional de Dados. Resolução CD/ANPD nº 19, de 23 de agosto de 2024. Disponível em https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396. Acesso em: 26 maio 2025.

Perfil de Empresa	Principais Desafios
Startups	Priorização do crescimento sobre a conformidade; ausência de estrutura jurídica interna; tratamento intensivo de dados desde o início
Microempresas e Empresas de Pequeno Porte	Escassez de recursos técnicos e financeiros; dificuldade em contratar especialistas; cobrança de conformidade por parte de grandes parceiros.
Grandes Empresas	Sistemas legados; descentralização de decisões; alta exposição reputacional; necessidade de reengenharia de processos.
Multinacionais	Conflito de legislações internacionais; exigências sobre transferências de dados; barreiras culturais; coordenação de políticas globais.

5. BOAS PRÁTICAS E ESTRATÉGIAS PROPORCIONAIS DE CONFORMIDADE

Diante da diversidade de perfis empresariais e do alto grau de complexidade regulatória, torna-se essencial adotar estratégias de conformidade que estejam de acordo com a realidade de cada organização, ou seja, é necessário reconhecer que a efetividade da proteção de dados não está necessariamente ligada ao porte da empresa, mas à sua capacidade de implementar medidas coerentes com os riscos aos quais está exposta. A seguir, são apresentadas boas práticas aplicáveis de forma adaptada a diferentes contextos.

5.1. Avaliação de Riscos como Ponto de Partida

Independentemente do tamanho da organização, um dos primeiros passos para a conformidade é a realização de um diagnóstico relacionado ao tratamento dos dados pessoais, cujo objetivo é mapear todas as atividades de tratamento, identificar as bases legais utilizadas, classificar os dados por categoria (comuns ou sensíveis), classificar os titulares por categorias, e analisar a existência de compartilhamento ou não das informações interna ou externamente – inclusive no tocante a transferências internacionais. A partir dessa análise, é possível priorizar os riscos mais críticos e definir medidas proporcionais de mitigação.

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) é uma ferramenta valiosa nesse processo. Apesar de ser obrigatória somente em determinadas situações, a realização voluntária do RIPD permite melhor compreensão dos riscos envolvidos durante o tratamento de algumas informações, especialmente quando envolvem o uso de tecnologias como biometria, IA e sistemas de pontuação comportamental, além de servir como evidência de diligência em caso de fiscalização pela ANPD[18].

5.2. Governança Responsiva e Multidisciplinar

A estruturação de um programa de governança em privacidade deve envolver diversas áreas da organização: jurídico, tecnologia da informação, segurança da informação, *compliance*, RH, marketing e produtos. A figura do encarregado pelo tratamento de dados desempenha papel central na articulação entre essas frentes, sendo responsável pela orientação interna, pelo apontamento de riscos, pela comunicação com os titulares e pelo relacionamento com a ANPD.

Empresas de menor porte podem adotar modelos mais enxutos, com uso de *templates* e *checklists* que auxiliem na gestão de consentimentos, atendimento a titulares e gestão de incidentes. Já empresas maiores e multinacionais, que podem investir em estruturas maiores e mais robustas, normalmente possuem Comitê de Privacidade e Proteção de Dados, indicadores de desempenho (KPIs), avaliação de maturidade anual, monitoramento do programa de privacidade e políticas segmentadas por área de negócio.

5.3. Documentação e Transparência

Um aspecto muitas vezes negligenciado, mas essencial quando falamos em conformidade regulatória, é evidenciar todas as decisões e medidas adotadas pela organização ao longo de sua atuação.

18. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Relatório de Impacto à Proteção de Dados Pessoais (RIPD). Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd. Acesso em: 27 maio 2025.