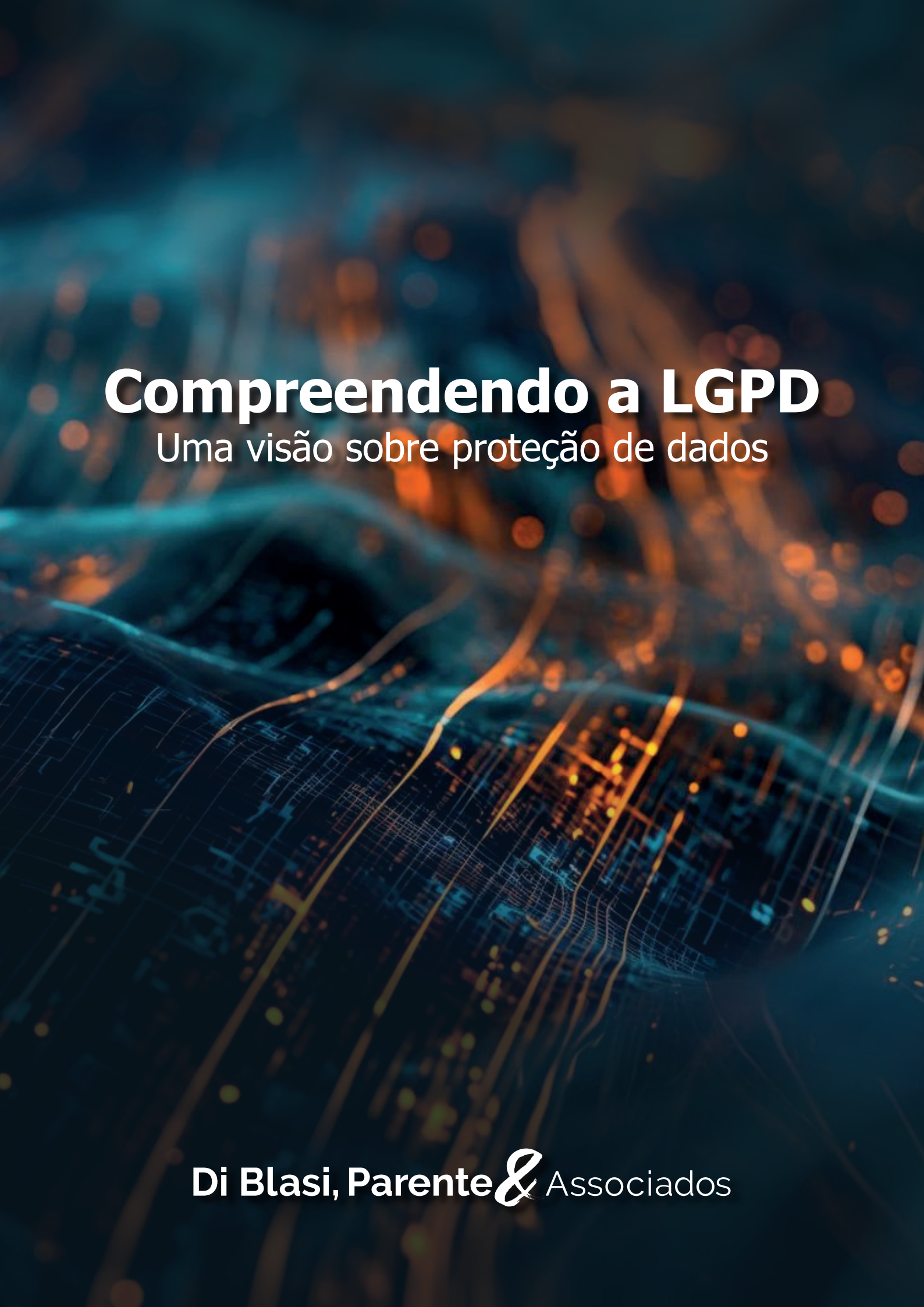

Compreendendo a LGPD
Uma visão sobre proteção de dados
Di Blasi, Parente & Associados

Histórico

A publicação da Lei Geral de Proteção de Dados (LGPD) foi um marco na legislação brasileira em relação à proteção de dados pessoais. Inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, a LGPD foi sancionada no Brasil em agosto de 2018. Sua criação se deu, principalmente, como resultado de uma abordagem preexistente em outros países, com relação à privacidade e à segurança dos dados pessoais, questões essenciais, em um mundo cada vez mais digital e comprometido com uma economia globalizada.

A Lei Geral de Proteção de Dados (LGPD) estabelece diversas exigências para as empresas que realizam o tratamento de dados pessoais e sejam eles simples ou sensíveis. Para que esse tratamento seja realizado, é necessário que haja respaldo legal em uma ou mais das seguintes bases legais:

- Consentimento
- Legítimo interesse
- Execução de contratos
- Processo judicial ou administrativo
- Obrigação legal ou regulatória
- Proteção à vida
- Tutela da saúde
- Realização de estudos por órgão de pesquisa
- Proteção do crédito
- Tratamento compartilhado de dados para execução de políticas públicas previstas em Leis ou regulamentos
- Garantia de prevenção a fraudes e segurança do titular

Além dessas regras, a legislação de proteção de dados pessoais elenca 10 princípios fundamentais que devem ser obrigatoriamente observados para o adequado tratamento desses dados:

1. Finalidade
2. Adequação
3. Necessidade
4. Livre acesso
5. Qualidade dos dados
6. Transparência
7. Segurança
8. Prevenção
9. Não discriminação
10. Responsabilização e prestação de contas

O cumprimento desses princípios é essencial para garantir a proteção dos direitos individuais e a confiança no uso de dados pessoais.

Momento atual

Atualmente, no Brasil, muitas empresas ainda se encontram em um momento de implementação e adaptação à LGPD. Algumas delas largaram na frente, e estão em uma fase mais adiantada, monitorando e/ou revisando procedimentos já implementados. A constante atualização dos programas de governança em privacidade é necessária, uma vez que novas regulações são a todo momento publicadas pela Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável por regulamentar, fiscalizar e orientar a aplicação da LGPD no país.

Desde janeiro de 2023 foi possível quantificar os tipos de incidentes de segurança comunicados à ANPD. Clique aqui e confira o Relatório de Ciclo de Monitoramento.

- Sequestro de dados (ramsonware) com transferência de informações: 40 comunicados
- Sequestro de dados (ramsonware) sem transferência de informações: 34 comunicados
- Exploração de vulnerabilidade em sistemas de informação: 24 comunicados
- Acesso não autorizado a sistemas de informação: 19 comunicados
- Roubo de credenciais: 9 comunicados

De acordo com o IT Trends Snapshot 2023, um estudo realizado pela Logicalis, uma empresa global de soluções e serviços de T.I., foram entrevistados 123 executivos de empresas brasileiras na área de tecnologia da informação. A pesquisa revelou que apenas 36% das empresas afirmaram estar em total conformidade com as regulamentações, o que já representa um aumento significativo em comparação com a pesquisa anterior, onde apenas 11% estavam em conformidade.

No entanto, uma parcela considerável de empresas (43%) ainda está na fase de implementação, com ações em andamento para se adequarem às regulamentações. Paralelamente a essa tendência, houve uma redução significativa no número de organizações que declararam não ter ações específicas para a LGPD. Na pesquisa de 2019, esse número era de 41%, diminuindo para 12% em 2021 e chegando a apenas 6% este ano.

No que diz respeito aos obstáculos para a conformidade com a LGPD, os participantes da pesquisa mencionaram desafios como adequação de processos/sistemas, engajamento de usuários/colaboradores, segurança de dados, mapeamento de processos, apoio da alta direção/prioridade, cultura da empresa, conhecimento da lei, fornecedores/tecnologias confiáveis, custos/investimentos e profissionais qualificados.

No mesmo estudo do IT Trends Snapshot 2023, também foi identificado que as principais iniciativas de T.I. em andamento, para as empresas se adequarem à LGPD, são lideradas pela redefinição dos processos de tratamento de dados, mencionada por 77% dos entrevistados, seguida pela adequação dos websites e portais (69%), mapeamento do ciclo de vida dos dados (67%) e implementação de novos processos e fluxos de trabalho em conformidade com a lei (62%), entre outras ações.

Ainda, segundo a pesquisa divulgada pelo Comitê Gestor da Internet no Brasil (CGI.br), apenas 28% das empresas fizeram alterações em contratos vigentes para adequação à LGPD. O que denota um dado também preocupante, uma vez que a adequação contratual estabelece responsabilidades, direitos e deveres entre as partes com relação ao tratamento de dados pessoais, durante e após a vigência contratual, tendo em vista a necessidade de definir as salvaguardas adequadas entre os parceiros de negócio, colaboradores e prestadores de serviços.

É fundamental estabelecer um diálogo constante e transparente, com a definição de garantias adequadas, previstas contratualmente, entre todos aqueles que utilizarão e compartilharão dados pessoais para o desenvolvimento das atividades empresariais.

Nesse contexto, além das medidas organizacionais e administrativas já implementadas, são necessários ainda investimentos em tecnologias de segurança e de proteção de dados para a garantia da confidencialidade, integralidade das informações e mitigação dos riscos de incidentes cibernéticos.

Com relação aos incidentes e vazamentos de dados pessoais, a Tenable, empresa americana especializada em gerenciamento de exposição cibernética, divulgou em 2023 um relatório do cenário de ameaças apontando que 984,7 milhões de dados foram vazados no Brasil no ano de 2022. Isso representa 112 terabytes de informações expostas no país, volume que representa 43% dos 257 terabytes em todo o mundo, de acordo com o relatório.

A IBM Security apresentou um Relatório de custos das violações de dados de 2023, onde foram analisadas mais de 550 organizações em todo o mundo que tiveram dados violados por ataques. O relatório IBM constatou que o custo médio global de uma violação de dados em 2023 foi de US$ 4,45 milhões, um aumento de 15% ao longo de 3 anos. Adicionalmente, 51% das organizações planejam aumentar os investimentos em segurança por conta de alguma violação que sofreram, incluindo planejamento e teste de resposta a incidentes (RI), treinamento de funcionários e ferramentas de detecção e resposta a ameaças. A economia média das organizações que utilizam amplamente a IA e a automação de segurança é de US$ 1,76 milhão em comparação com as organizações que não utilizam esses recursos.

Essa crescente onda de vazamentos de dados destaca a importância de medidas mais robustas de proteção e segurança cibernética, tanto por parte das empresas que armazenam informações pessoais, quanto por parte dos órgãos reguladores e do governo. A proteção adequada dos dados é essencial para garantir a privacidade e a segurança dos brasileiros em um mundo digital cada vez mais conectado e exposto a ameaças cibernéticas.

Assim fica claro que apesar do fato do grande volume de dados e informações tratados pelas organizações, inclusive dados pessoais sensíveis e informações confidenciais, algumas empresas, infelizmente, ainda não estão totalmente preparadas para mitigar os riscos e assegurar a proteção de dados pessoais, garantindo a devida privacidade do cidadão.

Sendo assim, todo esse processo de transição e adequação à LGPD inclui a definição de políticas claras e procedimentos internos de privacidade efetivos, bem como a revisão dos contratos de parceiros comerciais e a elaboração de novos documentos de governança em privacidade.

Contudo é essencial o fortalecimento de uma cultura de proteção de dados, por meio da conscientização e empoderamento dos funcionários e colaboradores, uma vez que as medidas de privacidade só serão efetivamente estabelecidas e implementadas, através de uma efetiva governança em privacidade aplicada na prática do dia a dia corporativo.

Tendência

Antes da LGPD, o Brasil carecia de uma legislação específica para regulamentar o tratamento de dados pessoais. A falta de regras claras e de um órgão regulador permitia práticas abusivas e a vulnerabilidade dos dados dos cidadãos. Por isso, a LGPD desempenha um papel fundamental na proteção da privacidade e na promoção da transparência no uso dos dados pessoais.

Além disso, as legislações de privacidade em todo mundo são cada vez mais relevantes e essenciais, e devem ser aplicadas e observadas em toda e qualquer atividade empresarial que trate dados pessoais.

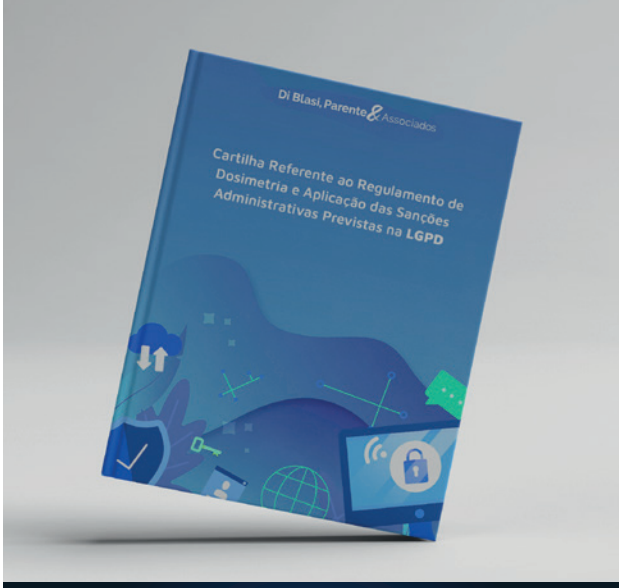
Nesse novo contexto, a sociedade tem um papel fundamental e, felizmente, está cada vez mais consciente da importância da privacidade e da segurança dos seus dados pessoais, o que de certa forma, pressiona as empresas a reforçarem a transparência e a adotarem medidas eficazes para assegurar a privacidade do cidadão.

A boa notícia é a tendência de um amadurecimento exponencial da cultura de proteção de dados no país. As empresas passaram a adotar a proteção de dados como parte de sua estratégia de negócios, incorporando-a em todos os níveis da organização. Isso inclui o desenvolvimento, aprimoramento e monitoramento dos programas de privacidade, com treinamentos contínuos, procedimentos de auditorias internas e a participação do encarregado de proteção de dados (DPO) na linha de frente do programa de governança da privacidade.

Além disso, é inevitável que a LGPD influencie na credibilidade e transparência dos serviços e produtos oferecidos pelas empresas. Não somente os consumidores, mas também todos os demais stakeholders envolvidos, exigirão cada vez mais o respeito à sua privacidade e ao tratamento adequado de seus dados pessoais. Com isso, as empresas que se adequarem às exigências da LGPD, de forma efetiva, saem na frente, construindo relações de confiança com seus clientes e parceiros de negócio, fortalecendo sua reputação e imagem no mercado.

As corporações devem ficar atentas aos princípios trazidos expressamente pela LGPD, como por exemplo, o princípio da finalidade, em que a realização do tratamento deverá alcançar propósitos legítimos, específicos, explícitos e informados ao titular, sem a possibilidade de tratamento posterior de forma incompatível com a finalidade previamente informada ao titular.

Essa atenção redobrada no tratamento dos dados pessoais também gera outros impactos positivos, e grandes oportunidades no mercado, seja para pensar em novos produtos e serviços, a partir do mapeamento e registro dos dados pessoais, na precificação de uma rodada de investimento ou em um processo de fusão e aquisição. Além disso, será possível vislumbrar novas medidas que garantam um sistema de prevenção e segurança que vise evitar ou responder mais rapidamente a incidentes cibernéticos.



Novas regras para a aplicação de multas e sanções administrativas pela ANPD e os seus impactos no Brasil (Clique na imagem acima e confira o nosso ebook sobre a dosimetria e aplicação das sanções com maior detalhamento sobre o tema)

Em 2023, a Autoridade Nacional de Proteção de Dados (ANPD) publicou um novo regulamento com regras para a dosimetria de multas e aplicação de sanções administrativas, em conformidade com as diretrizes da LGPD. As multas previstas na LGPD serão calculadas com base no faturamento da empresa, no seu último exercício, podendo chegar a 2% do faturamento anual, limitado a R$ 50 milhões de reais por infração.

Além disso, as sanções também podem incluir a publicação ostensiva da condenação, bloqueio do acesso a dados pessoais e até proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados.

A aplicação das novas regras pela ANPD ainda está apenas no começo, mas já é possível perceber que as empresas terão que redobrar a atenção na governança da privacidade e na implementação de boas práticas para garantir um adequado tratamento dos dados pessoais, e assegurar a confiança dos stakeholders.

Em um mundo cada vez mais digital, a privacidade se tornou um bem valioso e a proteção dos dados pessoais se tornou uma estratégia corporativa importante, além de ser uma obrigação legal. Portanto, as empresas precisam estar cientes das novas regras e se adaptar para evitar sanções rigorosas e/ou danos à reputação e imagem da organização.

A Autoridade Nacional de Proteção de Dados (ANPD) publicou em 8 de dezembro de 2023 o segundo Relatório de Ciclo de Monitoramento (RCM) da Coordenação-Geral de Fiscalização (CGF). O documento avalia as atividades do primeiro semestre de 2023, direcionando as estratégias orientativas, preventivas e repressivas da fiscalização. Também é um mecanismo de transparência, que reforça a preocupação da Autoridade em manter-se aberta à sociedade.

De acordo com o RCM, de janeiro a junho deste ano, a CGF recebeu 496 Requerimentos. Trata-se da soma das denúncias de violações à Lei Geral de Proteção de Dados Pessoais (LGPD) e das petições de titulares (solicitação de um titular de dados para exercer os seus direitos em relação ao tratamento de dados pessoais). A maior parte dos Requerimentos refere-se aos setores administração pública, telecomunicações, plataformas digitais, bancos, financeiras, administradoras de cartão e agregadores de dados.

Em dezembro de 2023, a Autoridade Nacional de Proteção de Dados (ANPD) também apresentou o Mapa de Temas Prioritários ("MTP") para o próximo biênio 2024/2025. O MTP delimita e prioriza as matérias para fins de estudo e planejamento das atividades de fiscalização da ANPD para o período de dois anos.

O MTP tem como finalidade trazer segurança regulatória e transparência quanto ao planejamento da atuação da ANPD. Além disso, segundo a ANPD, o documento é uma ferramenta de comunicação capaz de informar, de maneira objetiva e clara, as perspectivas de atuação do órgão fiscalizatório da autoridade para o corte temporal nele delimitado.

A ANPD utilizou como metodologia, para a definição das prioridades e elaboração do MTP, a análise de critérios específicos como o risco, a gravidade, a atualidade e a relevância do tema. Dessa forma, o MTP elenca os seguintes temas prioritários e respectivos objetivos:

Tema 1
Direitos dos titulares: realizar ações de fiscalização, especialmente de orientação e preventivas, no escopo do tratamento de dados realizado pelo Poder Público, por plataformas digitais, pelo setor financeiro e pelo setor de telecomunicações;

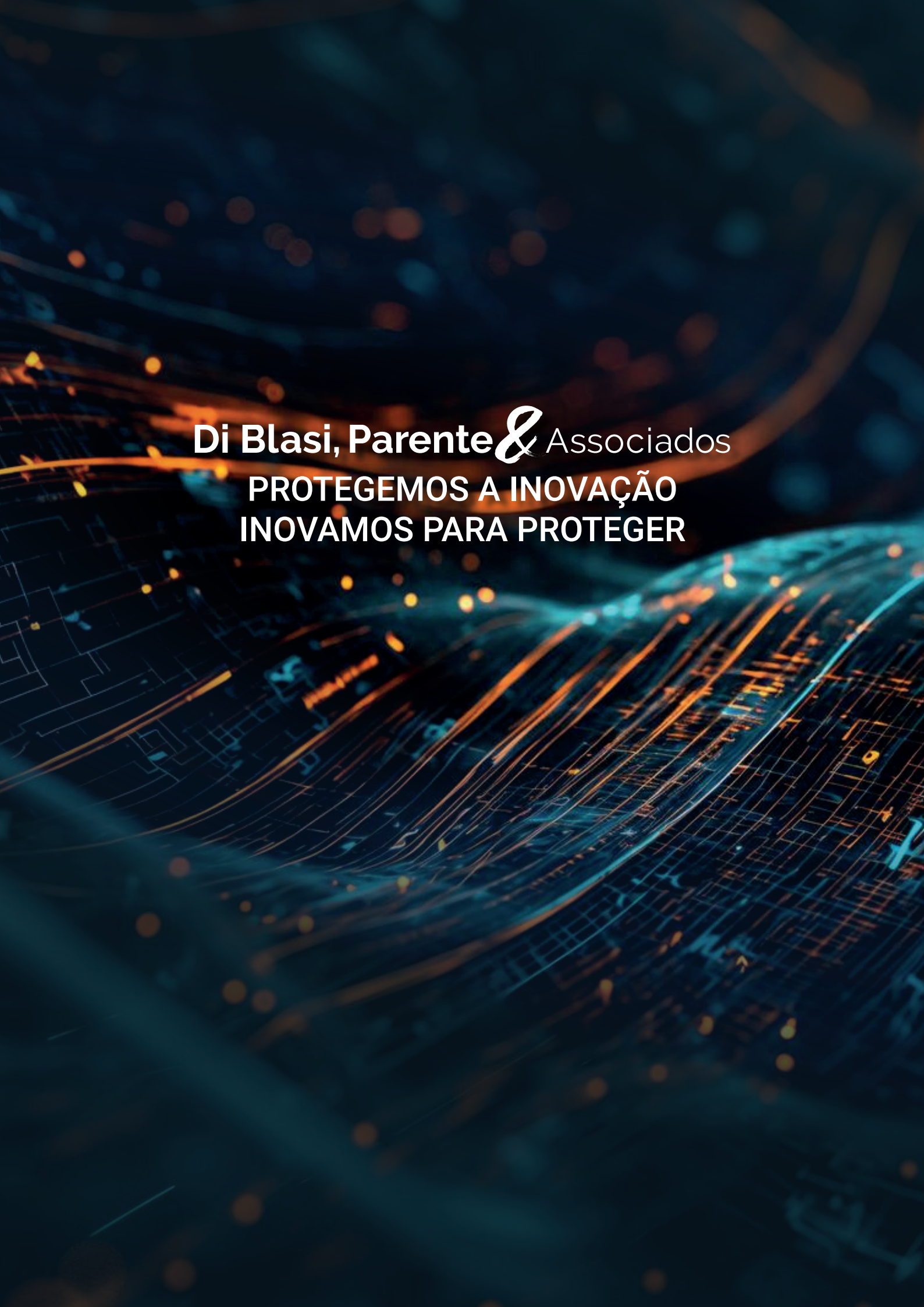
Tema 2
Tratamento de dados pessoais de crianças e adolescentes no ambiente digital: realizar ações de fiscalização para a salvaguarda dos direitos e assegurar a proteção de dados pessoais e o melhor interesse de crianças e adolescentes no ambiente digital;

Tema 3
Inteligência artificial para reconhecimento facial e tratamento de dados pessoais: identificar potenciais riscos no tratamento de dados pessoais no âmbito de sistemas de reconhecimento facial e assegurar o cumprimento da LGPD quanto ao tratamento de dados biométricos;

Tema 4
Raspagem de dados e agregadores de dados: verificar operações de tratamento para identificar a eventual necessidade de medidas cabíveis para adequações à LGPD.

Nossa equipe de Direito Digital e Proteção de Dados está acompanhando a evolução de todas as atividades e novas regulações da ANPD no Brasil. Caso deseje obter mais informações sobre o tema, acesse nosso site clicando aqui.

Fonte:
[1]https://dl.acm.org/doi/abs/10.1145/3439873
[2]https://imagine.la.logicalis.com/it-trends-snapshot-2023#form
[3]https://brasilpaisdigital.com.br/anpd-faz-balanco-da-lei-geral-de-protecao-de-dados-e-aponta-perspectivas-regulatorias-para-2024/


Di Blasi, Parente & Associados
PROTEGEMOS A INOVAÇÃO
INOVAMOS PARA PROTEGER