ESPECIAL

L.O. BAPTISTA 50 ANOS

5 TEMAS DE PRIVACIDADE E PROTEÇÃO DE DADOS

QUE MAIS SE DESTACARAM NOS 5 ANOS DA LGPD NO BRASIL

INTRODUÇÃO

A Lei Geral de Proteção de Dados (LGPD) completa seus cinco anos de existência e os direitos fundamentais de liberdade e privacidade das pessoas naturais no Brasil passaram a ser defendidos de maneira mais específica e restritiva.

Para comemorar mais um ano de LGPD no Brasil, a equipe de **Privacidade e Proteção de Dados** de L.O. Baptista Advogados preparou uma lista com os **5 assuntos que foram destaque em matéria de privacidade e proteção de dados no Brasil.**

Explore conosco as principais implicações da regulamentação da proteção de dados pessoais, incluindo os direitos dos titulares, os desafios enfrentados pelas empresas, bem como as consequências de violações que diretamente afetam as atividades comerciais de agentes e o mercado brasileiro. Igualmente, destacamos as tendências para o futuro da privacidade e proteção de dados no Brasil.

Boa leitura!

SUMÁRIO

5 Assuntos
de maior destaque em Privacidade e Proteção de Dados — 3

5 Evidências
que provam que a LGPD já ‘pegou’ — 8

5 Tendências
de mercado em Privacidade e Proteção de Dados — 11

5 Desafios
de adequação em Privacidade e Proteção de Dados — 14

5 Situações
de risco nas organizações — 17

5 ASSUNTOS

de maior destaque em Privacidade e Proteção de Dados

#1 REGULAMENTAÇÃO DE DADOS

Com a entrada em vigor da LGPD, em setembro de 2020, a ANPD passou a ser a autarquia responsável por regulamentar o tratamento de dados pessoais no país. Desde então, a Autoridade tem ganhado destaque ao publicar regulamentos, guias e notas técnicas para orientar os agentes de tratamento – controladores e operadores - em relação às normas vigentes.

Hoje, é perceptível a movimentação da ANPD para colocar em prática as regras da LGPD, com publicações de maior relevância sobre como orientações para o processo de:

- Comunicação de Incidente de Segurança (CSI)
- Guia de Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado
- Regulamento de aplicação da LGPD para agentes de tratamento de pequeno porte
- Formulário Modelo de Registro das Operações de Tratamento de Dados Pessoais para Agentes de Tratamento de Pequeno Porte (ATPP)
- Regulamento do Processo de Fiscalização e do Processos Administrativo Sancionador
- Regulamento de Dosimetria e Aplicação de Sanções Administrativas

#2 CONSENTIMENTO E TRANSPARÊNCIA

O consentimento e a transparência estão intrinsecamente relacionados no contexto da proteção de dados pessoais. Enquanto consentimento é uma das bases legais de tratamento, a transparência é um princípio que garante e informa a eficácia do uso desta base legal.

Sem a transparência, o consentimento é questionável.

Ao solicitar o consentimento do titular de dados, o controlador deve fornecer informações claras e compreensíveis sobre como seus dados pessoais serão usados, porque serão coletados, quem terá acesso a eles e por quanto tempo ficarão armazenados. É um processo de comunicação aberta e honesta com o titular de dados.

Do ponto de vista da empresa (controladora dos dados), a relação entre conceito e transparência é fundamental para construir confiança com os titulares, garantir a conformidade com a LGPD, demonstrar compromisso com a privacidade e como uma ferramenta de mitigação de riscos.

#3 DIREITOS DOS TITULARES DE DADOS

Os direitos dos titulares transcendem a proteção de informações. É claro que, ao observar e cumprir os preceitos da LGPD, os controladores garantem aos titulares diversos direitos, tais como o acesso aos seus dados, a correção de informações incompletas ou imprecisas, a revogação do consentimento e a exclusão dos seus dados pessoais. Esses direitos representam uma mudança significativa na forma como as organizações lidam com os dados pessoais de seus clientes, funcionários e parceiros comerciais, de modo a respeitar as informações pessoais dos titulares de dados.

Os direitos não correspondem apenas a salvaguardas jurídicas, mas catalisadores de inovação. Ao permitir que os titulares acessem, corrijam, revoguem e restrinjam seus dados, a LGPD incentiva empresas a criarem ecossistemas confiáveis e engajadores.

Em suma, a observância de tais direitos pelas empresas evita infrações e penalidades e fomenta o respeito à privacidade.

#4 PROTEÇÃO DE DADOS NAS RELAÇÕES DE TRABALHO

No universo das relações laborais, a proteção de dados é um tema de destaque sob a LGPD. Empresas e empregadores enfrentam o desafio de garantir o tratamento adequado dos dados pessoais de empregados celetistas, de modo a assegurar a privacidade de dados pessoais sensíveis e o cumprimento das exigências legais. Isso envolve obter consentimento dos colaboradores, garantir o acesso e compartilhamento apropriado de dados, bem como a implementação de políticas de privacidade internas.

A implementação de políticas internas de privacidade não é apenas um imperativo legal, mas antes uma medida de boa governança a evidenciar o comprometimento das empresas em proteger os direitos e a privacidade de seus colaboradores.

Ao adotar uma abordagem proativa para a proteção de dados nas relações de trabalho, as empresas evitam riscos legais e financeiros, cultivam um ambiente de confiança e respeito mútuo, todos fundamentais para o sucesso duradouro em um mundo cada vez mais centrado em dados.

#5 SEGURANÇA DE DADOS PESSOAIS E INCIDENTES DE SEGURANÇA

A segurança de dados pessoais, especialmente a cibernética, emerge como um dos temas protagonistas dentre os de maior relevância nas organizações.

Trata-se de questão crítica que evoluiu rapidamente, deixando de ser mera consideração técnica para um pilar essencial na confiança digital. Medidas mitigatórias para evitar incidentes de vazamento de dados passaram a servir como garantia de conformidade com a LGPD.

O **Brasil tem testemunhado aumento no número de ataques cibernéticos e violações de dados.**

103,16 bilhões de tentativas de ataques cibernéticos em **2022**

Notícias e pesquisas reforçam a importância de investir em medidas robustas de para evitar danos à reputação e penalidades por infração à LGPD, considerando o ininterrupto crescimento de vazamento de dados e sequestro digital.

A contratação de um seguro cyber cada vez mais sofisticado e a atenção minuciosa aos termos da apólice são elos fundamentais na corrente de segurança.

Tudo isto torna a segurança uma prioridade para empresas que desejam evitar multas e danos à reputação.

5 EVIDÊNCIAS

que provam que a LGPD já ‘pegou’

#1 DIREITOS COLETIVOS

Em decisão recente, um banco enfrentou uma condenação de R$10 milhões devido ao vazamento de dados de seus clientes, valor que foi reduzido para R$1,5 milhão após acordo firmado com o Ministério Público.

Além disso, em duas Ações Civis Públicas movidas por uma entidade da sociedade civil, uma conhecida rede social foi condenada este ano ao pagamento de uma multa milionária (R$ 20 milhões) pelo vazamento de dados pessoais em massa de seus usuários.

A decisão nesse caso enfatizou a importância de agentes de tratamento de assegurar proteção das informações dos usuários e alertou para as consequências severas de violações à privacidade no ambiente digital.

#2 ESFERA CÍVEL

Em um caso recente, o Tribunal de Justiça do Distrito Federal (TJDFT) decidiu manter condenação de primeira instância a empresas de telefonia que vazaram dados pessoais de consumidores de sua base. A decisão destacou que as operadoras tinham o dever de fornecer segurança aos dados pessoais de seus clientes disponibilizados na ocasião de contratação do serviço.

Na esfera cível os casos em que se discutem condenação por danos morais aos titulares de dados, pesquisas apontam um entendimento dos tribunais entre R$ 2mil e R$ 20mil, dependendo das características de cada situação.

#3 REPERCUSSÕES TRABALHISTAS

Casos envolvendo empregados demitidos por uso indevido de dados pessoais vêm cada vez mais à tona. Empregados acessaram e compartilharam informações sensíveis, levantando questões sobre a privacidade no ambiente de trabalho. Do mesmo modo, demissões por justa causa relacionadas à exposição indevida de conversas pessoais em aplicativos de mensagens destacam a importância do respeito à privacidade de empregados e prestadores de serviços.

Na esfera trabalhista os casos em que se discutem condenação por danos morais dos titulares de dados giram em torno de R$ 5mil.

#4 PROCONS DE MÃOS DADAS COM A LGPD

Órgãos de defesa do consumidor, como o Procon/MS e o Procon de São Paulo, têm atuado a favor da aplicação da LGPD em relações de consumo. Procon/MS autuou grandes sites e aplicativos de venda por infração à LGPD. Após fiscalização, o órgão constatou que as empresas praticavam termos de uso abusivos e políticas de privacidade e cookies em descumprimento com a LGPD. Em outro caso, o Procon de São Paulo (2022) aplicou uma multa em de R$ 572 mil a uma grande rede de drogarias em razão do uso irregular de dados de consumidores, que teria sido levado a cabo em violação à LGPD.

#5 COM A PALAVRA, A ANPD

Em um marco histórico, a Autoridade Nacional de Proteção de Dados (ANPD) aplicou sua primeira multa por descumprimento à LGPD em julho de 2023. Essa ação punitiva reforçou a relevância da agência reguladora no monitoramento e fiscalização das práticas de proteção de dados no país, sinalizando a seriedade das consequências para quem negligenciar as disposições da legislação de privacidade.

5 TENDÊNCIAS

do mercado em Privacidade e Proteção de Dados

#1 PRIVACIDADE COMO DIFERENCIAL COMPETITIVO

Empresas têm se movimentado para atender regras de proteção de dados não apenas da LGPD, mas também de outros importantes instrumentos normativos no mundo, como o GDPR (o Regulamento Geral de Proteção de Dados Pessoais da União Europeia), a CCPA (Lei de Privacidade do Consumidor da Califórnia, EUA), assim como normativas já vigentes mundo afora e que refletem nas relações internacionais.

O foco na privacidade é crescente, desde multinacionais até negócios locais. A seleção de fornecedores passou a incluir critérios de privacidade, transformando a conformidade em um diferencial competitivo e um requisito para relações comerciais sólidas.

#2 GOVERNANÇA DE INTELIGÊNCIA ARTIFICIAL

A crescente integração da Inteligência Artificial (IA) nos negócios impulsiona a necessidade de governança sólida.

Garantir que a IA atue em conformidade com a privacidade e proteção de dados se torna crucial.

Empresas passam a adotar abordagens estratégicas para supervisionar e controlar o uso responsável e ético dos dados, promovendo uma integração harmoniosa da IA com a conformidade regulatória. Da mesma forma, as pressões regulatórias no globo apontam para maior grau de explicabilidade dos algoritmos empregados no desenvolvimento de IA, e consequentemente, de proteção de dados pessoais em sistemas de tratamento baseados na tomada de decisão automatizada.

.

#4 DESIGNAÇÃO DE ENCARREGADO DE PROTEÇÃO DE DADOS (DPO)

A figura do DPO evolui como catalisador da privacidade e proteção de dados nas organizações.

A escolha de um DPO confiável e capacitado é fundamental para integrar a conformidade à cultura organizacional, estimulando de forma construtiva um ambiente em que a privacidade e proteção de dados sejam parte orgânica do negócio e não algo impeditivo ou um tabu.

Como tendência, organizações que não possuem departamento interno dedicado estão buscando consultorias especializadas para orientação contínua e garantia de interação eficaz com titulares de dados e a ANPD.

#5 CONSUMIDORES MAIS EXIGENTES

A conscientização do público sobre privacidade está crescendo, resultando em consumidores mais informados e exigentes. Empresas são avaliadas não apenas pela qualidade de seus produtos e serviços, mas também por como lidam com dados pessoais.

A transparência e o compromisso com a proteção de dados são agora fatores de influência nas escolhas dos consumidores, impactando diretamente a reputação e o sucesso dos negócios.

5 DESAFIOS

de adequação em Privacidade e Proteção de Dados

#1 TRADUÇÃO DE MODELOS DE GOVERNANÇA EM PROCESSOS OPERACIONAIS SÓLIDOS

Transformar os modelos de governança de privacidade em processos operacionais consistentes é um passo fundamental para garantir a conformidade contínua.

Isso requer a integração das diretrizes de privacidade em todas as operações da organização, desde a coleta de dados até o seu processamento e compartilhamento, assegurando que cada ação esteja alinhada com os princípios regulatórios.

#2 MONITORAMENTO ESTRATÉGICO DE FORNECEDORES E PARCEIROS DE NEGÓCIOS

Selecionar parceiros e fornecedores em conformidade com regulamentações de privacidade é crucial, especialmente em cadeias de suprimentos complexas.

> O monitoramento ativo dessas entidades garante que os dados compartilhados estejam protegidos ao longo de toda a colaboração, minimizando riscos e promovendo uma cultura de confiança no ecossistema de negócios.

#3 TRANSFERÊNCIA INTERNACIONAL DE DADOS EM UM MUNDO GLOBALIZADO

Operar globalmente implica na transferência de dados entre jurisdições, o que pode ser desafiador devido a diferentes leis de privacidade.

Estratégias para cumprir com regulamentações internacionais, como acordos contratuais e garantias adicionais, tornam-se essenciais para garantir que os dados pessoais sejam tratados com a devida proteção em todas as fronteiras.

#4 EDUCAÇÃO E CONSCIENTIZAÇÃO CONSTANTES

Estabelecer uma cultura de privacidade exige educação e treinamento contínuos. Enquanto equipes técnicas têm familiaridade com o tema, outras áreas como RH, comercial e marketing precisam receber treinamentos recorrentes para alinhar seus fluxos de trabalho com as políticas de privacidade.

A capacitação não apenas fortalece a compreensão, mas também garante que os processos internos sejam executados conforme planejado.

#5 ENGAJAMENTO EFETIVO DA ALTA DIREÇÃO

O comprometimento da alta direção é fundamental. Criar uma cultura organizacional sensível à privacidade requer o envolvimento ativo dos líderes, que devem demonstrar apoio constante e alinhar estratégias de privacidade aos objetivos da empresa.

Sua liderança estabelece um exemplo que permeia todos os níveis da organização.

5 SITUAÇÕES
de risco nas' Organizações

#1 RESPONSABILIDADE SOLIDÁRIA

A LGPD estabelece a responsabilidade solidária, entre os controladores e operadores e as cláusulas contratuais serão o norte na hipótese de incidentes. Uma cláusula bem escrita é capaz até mesmo de eximir uma das partes da responsabilidade. É comum que as organizações já possuam regras com seus parceiros de negócios em relação as responsabilizações, como nos casos de vínculos empregatícios, garantias de produtos, lei anticorrupção.

O mesmo pode ser definido para responsabilidades decorrentes do tratamento de dados pessoais, desde que aplicadas ao caso concreto sem repetição de clausulados padrões que não façam o menor sentidos para as relações estabelecidas entre as partes contratantes.

#2 TRABALHO HÍBRIDO E PROTEÇÃO DE REDES

O ambiente de trabalho híbrido traz desafios únicos à proteção de dados, especialmente relacionados à segurança de redes. A flexibilidade do trabalho remoto exige medidas rigorosas para proteger o acesso a dados sensíveis e garantir a conformidade com a LGPD. Adotar estratégias robustas de segurança cibernética e controlar o acesso à rede são fundamentais para evitar riscos potenciais.

#3 SITUAÇÕES CONSIDERADAS DE ALTO RISCO

Em 2022, a ANPD sinalizou critérios gerais e critérios específicos para os casos de tratamento de dados pessoais de alto risco (Resolução nº 2 regulamentando a aplicação para agentes de tratamento de pequeno porte), sinalizando a necessidade orientar o tratamento desses dados pela elaboração de Relatórios de Impacto à Proteção de Dados Pessoais (“RIPD”, já exigido por lei, como no art. 38 da LGPD).

Também é exigida a adoção de medidas, salvaguardas e mecanismos de mitigação de riscos potencialmente nocivos à garantia dos direitos fundamentais, tais como criptografia de dados e controle de acesso ao banco de dados, eliminação ou minimização e adoção de medidas para garantir proteção de dados.

#4 CANAIS INACESSÍVEIS PARA TITULARES DE DADOS

A ANPD já sinalizou sua atuação terá forte apelo também para a relação entre o titular do dado e o controlador sob a ótima da relação de consumo, sendo que a ausência de canais de comunicação para estes titulares possa exercer os direitos será causa flagrante de infração à LGPD.

Portanto, manter canais de comunicação acessíveis e intuitivos para titulares de dados é uma prioridade. Além disso, garantir que políticas e avisos de privacidade sejam facilmente compreensíveis e disponíveis para todos os públicos é fundamental, com o uso de estratégias de legal design para otimizar essa comunicação.

#5 FALHA NO PLANO DINÂMICO DE RESPOSTA A INCIDENTES

Uma equipe destreinada por causar um prejuízo ainda mais na hipótese de ocorrência de um incidente de segurança, até mesmo nos programas de governança em privacidade de dados mais estruturados e para as organizações com as melhores tecnologias implantadas. Por isto, ter um plano de resposta a incidentes é essencial, mas também é crucial que ele seja dinâmico e esteja em constante aprimoramento por parte das organizações.

O treinamento contínuo das equipes é vital para a rápida identificação de violações de dados pessoais, permitindo uma implementação eficaz do plano em situações dinâmicas e desafiadoras.

Nossa equipe de **Privacidade e Proteção de Dados** está à disposição para prestar esclarecimentos e orientações sobre o assunto.

Coautoria de: Denise A. Berzin Reupke

CONTATO

Esther Jerussalmy Cunha
Sócia
ejc@baptista.com.br

Fabrício B. Pasquot Polido
Sócio
fbp@baptista.com.br

L.O. BAPTISTA