GOVERNANÇA CORPORATIVA, LGPD E COMPLIANCE

AULA 6

Profª Neide Borscheid Mayer

CONVERSA INICIAL

A nova visão da gestão das organizações traz, por meio da governança corporativa, uma perspectiva de longo prazo que valoriza o desenvolvimento sustentável. Isso é alcançado pela implementação de um conjunto de práticas e políticas que guiam a conduta com base nos princípios de integridade, transparência, equidade, responsabilização e sustentabilidade.

Dentro deste contexto, o compliance emerge como uma função crucial para garantir que as empresas estejam em conformidade com leis, regulamentos e normas, tanto internas quanto externas.

No contexto da evolução das práticas de compliance, destaca-se a Lei Geral de Proteção de Dados (LGPD), que trata da proteção de dados pessoais e da privacidade de todos os stakeholders. Este último aspecto será explorado mais detalhadamente a seguir.

CONTEXTUALIZANDO

A Lei Geral de Proteção de Dados (LGPD – Lei n. 13.709, de 14 de agosto de 2018) é uma legislação brasileira que entrou em vigor para estabelecer regras sobre “o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou jurídica, de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural” (art. 1º).

A vigência desta lei teve um impacto significativo nas empresas brasileiras, exigindo uma mudança na forma como coletam, armazenam e utilizam dados pessoais de todas as pessoas com as quais se relacionam.

Para se adequarem às disposições da LGPD, as empresas precisaram investir em tecnologia, treinamento de funcionários e, frequentemente, contratar especialistas em proteção de dados. Isso porque, caso não se adequassem, estariam sujeitas a riscos de multas elevadas, danos à reputação e perda de confiança por parte de clientes e parceiros de negócios.

Dado que a implementação desta regulamentação ainda é considerada relativamente recente, exigindo mudanças tanto estruturais e tecnológicas quanto culturais, o Brasil continua sendo um dos países com maior número de vazamentos de dados no mundo. Isso demonstra a importância de aprimorar os

processos de proteção de dados e privacidade dos indivíduos, além de disseminar o conhecimento para que os próprios usuários possam se proteger desses riscos.

TEMA 1 – FUNDAMENTOS DO SISTEMA BRASILEIRO DE PROTEÇÃO DE DADOS PESSOAIS

A Lei Geral de Proteção de Dados Pessoais (LGPD – Lei n. 13.709/2018), em vigor no Brasil, foi inspirada na General Data Protection Regulation (GDPR), da União Europeia, e tem como objetivo proteger os dados pessoais de pessoas naturais, ou seja, pessoas físicas (colaboradores, clientes, fornecedores, sócios etc.) (Garcia, 2020).

Essa legislação não abrange a proteção de dados de empresas ou organizações (pessoas jurídicas), nem se aplica aos dados tratados por uma pessoa natural sem finalidade econômica, como em casos de uso para fins artísticos, jornalísticos e acadêmicos (Garcia, 2020). Da mesma forma, não envolve dados utilizados para segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão a infrações penais, para os quais há legislação específica (Garcia, 2020).

Essa legislação se tornou necessária diante da transformação digital em curso na sociedade, onde a coleta e o uso de dados pessoais se tornaram comuns pelas empresas nos diversos canais de comunicação e relacionamento estabelecidos com os stakeholders.

A LGPD visa proteger os dados pessoais das pessoas físicas com base nos fundamentos apresentados em seu art. 2º:

I. Respeito à privacidade: a legislação aborda o uso de dados de outra pessoa sem seu consentimento para qualquer finalidade. Garcia (2020) exemplifica isso com a publicação de dados de um indivíduo em uma rede social; mesmo que a postagem seja pública, isso não autoriza o uso indiscriminado por terceiros. Para utilizar os dados de outra pessoa, é necessário observar os princípios estabelecidos por esta lei.
II. Autodeterminação informativa: significa que o titular dos dados tem o direito de decidir sobre a utilização de seus dados pela empresa e os fins para os quais podem ser utilizados.

III. Liberdade de expressão, informação, comunicação e opinião;
IV. Inviolabilidade da intimidade, da honra e da imagem;
V. Desenvolvimento econômico e tecnológico e inovação;
VI. Livre iniciativa, livre concorrência e defesa do consumidor;
VII. Direitos humanos, livre desenvolvimento da personalidade, dignidade e exercício da cidadania pelas pessoas naturais.

Os fundamentos mencionados na LGPD reconhecem a importância dos dados na sociedade atual. Esses dados, quando associados à massa de informações de outros indivíduos, podem gerar insights estratégicos valiosos tanto para empresas quanto para governos, o que os torna altamente desejados e valorizados. Esse interesse massivo destaca a necessidade de proteção dos stakeholders, garantindo que seus dados sejam utilizados apenas conforme permitido pela legislação.

Os dados, por si só, são apenas elementos brutos sem significado ou contexto. Por exemplo, apresentar um número aleatório como 10 não representa mais do que um dado, pois carece de interpretação ou valor analítico.

No entanto, quando esses dados são processados, organizados e combinados com outros, eles se transformam em informações. Utilizando o mesmo exemplo do número dado, se mencionarmos “10 km por litro de combustível”, agora temos um contexto claro de consumo de combustível, indicando que um determinado veículo pode percorrer 10 quilômetros com apenas um litro de combustível. O dado inicial se converteu em informação, que, por sua capacidade de gerar conhecimento útil e significativo, pode orientar decisões estratégicas.

Em relação aos conceitos definidos pela LGPD e à interpretação correta dessas definições, a lei no art. 5º define:

- Dado pessoal: informações que identificam ou podem identificar uma pessoa física, como fotografia, CPF, RG, e-mail, número de telefone, entre outros.
- Dado pessoal sensível: refere-se a informações sobre origem racial ou étnica, convicções religiosas, opiniões políticas, filiação a sindicatos, saúde, vida sexual, dados genéticos ou biométricos, quando associados a uma pessoa natural.

- Dado anonimizado: dados de uma pessoa natural que não podem ser identificados, obtidos por meio de tecnologias disponíveis e adequadas na época do tratamento dos dados.

No mesmo art. 5º, a LGPD define os papéis das principais partes relacionadas ao processo de proteção de dados. Deve-se compreender que: o titular é a pessoa (natural) a quem os dados pertencem; o controlador é a pessoa (física ou jurídica) responsável pelas decisões referentes ao tratamento de dados pessoais, ou seja, quem deve seguir a legislação para não utilizar os dados do titular de maneira inadequada; o operador é a pessoa (física ou jurídica) que realiza o tratamento dos dados do titular em nome do controlador; o encarregado de dados é a pessoa que atua, em nome do controlador, como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); e a ANPD é o órgão do governo responsável por zelar, implementar e fiscalizar o cumprimento da LGPD no Brasil.

Considerando a relevância do tema para todas as organizações e o volume muito grande de dados pessoais que inevitavelmente são coletados pelas empresas, é fundamental que estas estabeleçam políticas e processos claros para proteção desses dados pessoais. Isso inclui definir como essas informações devem ser coletadas, armazenadas e compartilhadas.

A conformidade com a LGPD e as políticas e processos das organizações são responsabilidade de todos os stakeholders.

TEMA 2 – PRINCÍPIOS E CONCEITOS FUNDAMENTAIS NA LGPD

Como visto até o momento, o escopo da LGPD abrange a proteção de dados pessoais no tratamento dado a esses dados por pessoas físicas e jurídicas.

O tratamento de dados pode ser entendido como qualquer atividade que utilize um dado pessoal, incluindo operações como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle da informação, modificação, comunicação, transferência, difusão ou extração de dados (TJSP).

Um exemplo comum de coleta é quando uma empresa solicita um e-mail para enviar promoções. Portanto, o conceito de tratamento de dados na LGPD é abrangente, englobando qualquer operação que envolva dados pessoais em todo o seu ciclo de vida, desde a coleta até o descarte. Isso significa que simplesmente acessar, excluir ou manter um dado pessoal armazenado, mesmo que não utilizado, já é considerado atividade de tratamento de dados (Get Privacy).

Assim, a LGPD estabelece no art. 6º que toda atividade de tratamento de dados pessoais deve ser realizada com boa-fé e em conformidade com os seguintes princípios:

I. Finalidade: o tratamento deve ser realizado para fins legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com esses propósitos (art. 6º da Lei n. 13.709/2018). Isso implica que empresas e pessoas físicas que realizam qualquer tipo de tratamento de dados pessoais devem informar ao titular qual será a finalidade desse dado. Esse dado não pode ser utilizado para finalidades diferentes daquelas informadas e autorizadas pelo titular.

II. Adequação: o tratamento deve ser compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento (art. 6º da Lei n. 13.709/2018). Assim como é necessário respeitar a finalidade autorizada pelo titular para o tratamento de dados, o contexto de utilização desses dados também deve estar alinhado com o que foi originalmente informado. Portanto, as empresas devem utilizar os dados de acordo com os propósitos claramente definidos e comunicados, de forma coerente com as expectativas do titular.

III. Necessidade: “limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados” (art. 6º da Lei n. 13.709/2018). Esse princípio estabelece que os dados de terceiros devem ser obtidos e tratados apenas na quantidade e forma necessárias para cumprir a finalidade específica. Por exemplo, em uma compra à vista, a empresa precisa coletar e tratar apenas os dados necessários para emitir a nota fiscal, como nome e CPF, junto com

a informação do método de pagamento. Em muitos casos, no entanto, as empresas coletam um cadastro completo, incluindo dados como data de nascimento e endereço, sem explicar ao cliente (titular) o motivo dessa coleta e armazenamento, mesmo que esses dados não sejam essenciais para a finalidade de realizar a venda do item em questão. Isso exemplifica a não conformidade com o princípio da necessidade estabelecido pela LGPD.

IV. Livre acesso: “garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais” (art. 6º da Lei n. 13.709/2018). O livre acesso deve ser concedido a todas as pessoas naturais cujos dados são tratados por terceiros (pessoas físicas ou jurídicas). No exemplo anterior, qualquer empresa que tenha recebido dados do cliente deve permitir que ele consulte seus dados armazenados e informe por quanto tempo esses dados serão mantidos.

V. Qualidade dos dados: “garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento” (art. 6º da Lei n. 13.709/2018). Os dados devem ser precisos, claros, relevantes e atualizados, pois são fundamentais para tomada de decisões e para o cumprimento das finalidades estabelecidas. Portanto, quem realiza o tratamento dos dados tem a responsabilidade de assegurar essa qualidade. Além do direito de acessar seus dados, o titular também pode solicitar a exclusão ou correção dessas informações quando necessário.

VI. Transparência: “garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial” (art. 6º da Lei n. 13.709/2018). O princípio da transparência está diretamente relacionado aos princípios de livre acesso e qualidade dos dados, podendo ser categorizado em dois tipos: transparência ativa e transparência passiva. A transparência ativa refere-se à obrigação das empresas de divulgar informações de maneira proativa, sem que haja necessidade de solicitação por parte dos titulares dos dados. Isso inclui a divulgação regular de informações relevantes sobre o tratamento de

dados pessoais, como políticas de privacidade, propósitos do tratamento, direitos dos titulares e medidas de segurança adotadas. Já a transparência passiva envolve a disponibilização de informações específicas em resposta às solicitações dos titulares dos dados. Nesse caso, as empresas devem garantir o atendimento detalhado e preciso das solicitações, incluindo acesso, correção, exclusão de dados conforme requerido, além de informações sobre compartilhamento de dados, se houver.

VII. Segurança: “utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão” (art. 6º da Lei n. 13.709/2018). Em relação a esse princípio, as organizações devem implementar políticas, normas e procedimentos para garantir a segurança efetiva dos dados, prevenindo vazamentos e fraudes no uso inadequado dos dados.

Algumas boas práticas recomendadas para assegurar a segurança dos dados, conforme o Guia de Boas Práticas: Lei Geral de Proteção de Dados (LGPD), especialmente no que se refere ao armazenamento de dados, são apresentadas a seguir:

> • Criptografia: a utilização de algoritmos de criptografia é essencial para garantir a confidencialidade dos dados. Esse método transforma os dados em um formato ilegível para terceiros, a menos que sejam corretamente descriptografados, protegendo assim os dados contra leitura não autorizada.
>
> • Controle de acesso: o acesso aos dados deve ser restrito apenas a pessoas autorizadas. Isso requer a implementação de controles como senhas seguras, autenticação em dois fatores, entre outras medidas.
>
> • Backup e redundância: é crucial que o armazenamento de dados inclua mecanismos de backup e redundância para assegurar a disponibilidade contínua dos dados, mesmo em caso de falhas ou incidentes.
>
> • Controle de versões: a gestão das versões dos dados armazenados é fundamental para preservar a integridade e autenticidade das informações, além de permitir a rastreabilidade de alterações realizadas ao longo do tempo. (Brasil, 2020)

É importante também realizar capacitação e conscientização contínuas de todos os stakeholders sobre esses normativos, procedimentos, e o papel e responsabilidade de todos em relação à segurança dos dados.

VIII. Prevenção: “adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais” (art. 6º da Lei n. 13.709/2018). O princípio da prevenção está diretamente relacionado à gestão de riscos envolvendo o tratamento de dados, exigindo que as empresas atuem de forma preventiva na sua mitigação. Isso inclui desde a identificação dos riscos até a implementação de medidas preventivas e monitoramento contínuo.

Na fase de identificação dos riscos, as empresas devem avaliar o impacto potencial dos riscos, analisar a vulnerabilidade aos mesmos (ou seja, se as medidas de segurança adotadas são adequadas para mitigar o risco) e mapear todos os dados pessoais coletados, processados e armazenados.

Com base na identificação dos riscos, as empresas devem implementar medidas preventivas para mitigar esses riscos. Isso envolve a adoção de políticas e procedimentos de segurança da informação, o uso de tecnologias como criptografia, firewalls e sistemas de detecção de intrusões para proteger os dados pessoais contra acessos não autorizados, treinamento e conscientização sobre a importância da proteção de dados e práticas de segurança, além da implementação de controles de acesso rigorosos para garantir que apenas pessoas autorizadas tenham acesso aos dados pessoais.

A LGPD também requer, por meio do princípio da prevenção, que as empresas monitorem continuamente suas medidas de segurança e realizem ajustes quando necessário. Isso inclui auditorias regulares de segurança da informação para identificar e corrigir possíveis riscos ou vulnerabilidades, revisões periódicas e atualizações das políticas e procedimentos de proteção de dados para refletir mudanças nas regulamentações ou no ambiente de risco, e a criação e teste de planos de resposta a incidentes para lidar rapidamente com violações de dados ou incidentes de segurança.

IX. Não discriminação: “impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos” (art. 6º da Lei n. 13.709/2018). Esse princípio estabelece que as empresas devem tratar os dados pessoais de forma justa e equitativa, garantindo que o tratamento de dados não resulte em discriminação ou prejuízo aos titulares dos dados. Isso promove a igualdade e o respeito aos direitos fundamentais de todos os indivíduos. Um exemplo de violação desse princípio seria a coleta de dados durante

processos de seleção e contratação que poderiam levar a práticas discriminatórias, como solicitar um exame de gravidez a candidatas mulheres, por exemplo.

X. Responsabilização e prestação de contas: “demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas” (art. 6º da Lei n. 13.709/2018). Por meio desse princípio, a LGPD atribui aos agentes a responsabilidade pelo controle e gerenciamento dos dados pessoais e pela eficácia de todas as medidas adotadas nesse processo.

Em caso de identificação de alguma inconformidade e do não cumprimento dessa legislação, os agentes (aqueles que estão tratando dados pessoais de terceiros) estão sujeitos às sanções previstas no art. 52º da LGPD. Essas sanções são aplicadas conforme o resultado de processos administrativos, levando em consideração critérios como a gravidade e a natureza das infrações, os direitos pessoais afetados, a boa-fé do infrator, a vantagem auferida ou pretendida pelo infrator, a condição econômica do infrator, a reincidência, o grau do dano, a cooperação do infrator, a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, a adoção de política de boas práticas e governança, a pronta adoção de medidas corretivas, e a proporcionalidade entre a gravidade da falta e a intensidade da sanção (art. 52º, parágrafo 1º da Lei n. 13.709/2018).

As penalidades previstas pela LGPD para as empresas que descumprirem as regras vão desde uma advertência até a proibição parcial ou total das atividades que envolvem o tratamento de dados. Isso pode incluir a descontinuidade das operações da empresa, conforme destacado no art. 52º da Lei n. 13.709/2018:

> I – advertência, com indicação de prazo para adoção de medidas corretivas;
>
> II – multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
>
> III – multa diária, observado o limite total a que se refere o inciso II;

> IV – publicização da infração após devidamente apurada e confirmada a sua ocorrência;
>
> V – bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
>
> VI – eliminação dos dados pessoais a que se refere a infração;
>
> VII – suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
>
> VIII – suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
>
> IX – proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados.

Considerando a relevância e o alto impacto do descumprimento da LGPD pelas organizações, o tema do tratamento de dados é considerado um fato estratégico e fundamental. Portanto, o investimento em estruturas adequadas de recursos tecnológicos, normativos e procedimentais é essencial. Cada vez mais, as boas práticas de governança e a implementação de programas de compliance são fatores-chave na gestão de qualquer tipo de negócio.

TEMA 3 – REQUISITOS PARA O TRATAMENTO DE DADOS PESSOAIS E DIREITOS DO TITULAR

Como vimos até o momento, a LGPD se aplica a qualquer tipo de tratamento de dados realizado no Brasil, em qualquer meio (inclusive digital), por pessoa natural ou por pessoa jurídica, de direito público ou privado, que tenha como objetivo a oferta ou o fornecimento de bens ou serviços, ou o tratamento de dados de indivíduos localizados no território nacional, cujos dados pessoais utilizados no tratamento tenham sido coletados no território nacional (art. 1º e art. 3º da Lei n. 13.709/2018). Somente não serão considerados por essa legislação os casos previstos no art. 3º da LGPD que já foram apresentados anteriormente.

No capítulo II da LGPD são apresentadas as condições e situações em que o tratamento de dados pessoais pode ser realizado. A primeira condição apresentada é a necessidade de haver o consentimento do titular dos dados para o tratamento dos mesmos (art. 7º da Lei n. 13.709/2018). Esse consentimento

deve ser fornecido pelo titular por escrito ou por outro meio que demonstre a manifestação de vontade do titular (art. 8º, parágrafo 1º da Lei n. 13.709/2018).

Como exemplo desse consentimento, podemos mencionar o acesso às páginas de internet, sejam de notícias ou de empresas, por exemplo. Você já deve ter notado que muitas vezes, ao acessar determinada página, aparece na tela um pop-up solicitando o aceite dos cookies. Ao aceitar, o usuário está consentindo o tratamento de determinado dado pessoal relacionado ao acesso realizado.

O controlador (empresa ou pessoa física) que realizará o tratamento dos dados deve manter as evidências de que houve o consentimento do titular para esse tratamento (art. 8º, parágrafo 2º, da Lei n. 13.709/2018). A validade do consentimento é crucial para a conformidade com a LGPD, e ele deve ser fornecido de maneira livre, informada, inequívoca e específica. Caso seja evidenciado o que a LGPD chama de vício de consentimento, o tratamento de dados pessoais não pode ser realizado (art. 8º, parágrafo 3º e parágrafo 4º, da Lei n. 13.709/2018).

E o que seria um vício de consentimento? É quando o consentimento é obtido de forma inadequada e, por isso, não é considerado válido. Isso pode ocorrer se o consentimento for enganoso, abusivo, ou se as informações sobre o tratamento não forem apresentadas de forma prévia, transparente, clara e inequívoca. Exemplos dessas situações incluem casos em que o consentimento é forjado, obtido por meio de coação, ou quando é genérico ou contém informações insuficientes.

O consentimento concedido pelo titular pode ser revogado a qualquer momento, caso este se manifeste de forma expressa. O processo de revogação do consentimento deve ser gratuito e facilitado (art. 8º, parágrafo 5º da Lei n. 13.709/2018).

Outra condição para que o tratamento de dados pessoais possa ser realizado é nos casos de cumprimento de obrigação legal ou regulatória pelo controlador (art. 7º da Lei n. 13.709/2018). Este é o caso dos dados necessários para a emissão de nota fiscal em alguma venda realizada pela empresa, por exemplo.

A administração pública também poderá realizar o tratamento e o uso compartilhado de dados necessários à execução de políticas públicas previstas

em leis e regulamentos (art. 7º da Lei n. 13.709/2018). Para essa situação, podemos citar o tratamento de dados realizados (e compartilhados) pela Receita Federal e pelo INSS para o cumprimento das atividades de fiscalização, por exemplo.

As demais situações que permitem o tratamento de dados pessoais, segundo a LGPD (art. 7º da Lei n. 13.709/2018), são:

IV. para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
V. quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
VI. para o exercício regular de direitos em processo judicial, administrativo ou arbitral;
VII. para a proteção da vida ou da incolumidade física do titular ou de terceiro;
VIII. para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
IX. quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
X. para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Lembrando que a legislação estabelece de forma expressa que o titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados (art. 9º da Lei n. 13.709/2018). Essas informações devem ser disponibilizadas de forma clara, adequada e ostensiva, envolvendo, entre outros aspectos, a finalidade específica do tratamento, a forma e duração do tratamento, a identificação do controlador, as informações de contato do controlador, as informações acerca do uso compartilhado de dados pelo controlador e a finalidade, as responsabilidades dos agentes que realizarão o tratamento e os direitos do titular (art. 9º da Lei n. 13.709/2018).

Caso o controlador ou o operador que realizaram a atividade de tratamento de dados pessoais causem dano patrimonial, moral, individual ou coletivo ao titular do dado pessoal por não seguir as determinações da LGPD, são obrigados a repará-lo (art. 42º da Lei n. 13.709/2018).

TEMA 4 – GOVERNANÇA EM PROTEÇÃO DE DADOS: PROGRAMA DE PRIVACIDADE E RESPOSTA A INCIDENTES

Diante da importância e complexidade da implementação de políticas e procedimentos necessários para atender aos requisitos da LGPD, as entidades que realizam o tratamento de dados pessoais de terceiros (controladores e operadores) devem adotar boas práticas de governança dessas atividades (art. 50º da Lei n. 13.709/2018). Essas boas práticas abrangem uma ampla gama de aspectos, desde a organização e funcionamento até os procedimentos de reclamação e petição dos titulares, normas de segurança, padrões técnicos e obrigações específicas para os envolvidos no processo.

Para a elaboração desses processos e normativos, devem ser considerados a natureza, o escopo, a finalidade, bem como a probabilidade e gravidade dos riscos e benefícios associados ao tratamento de dados do titular. Além disso, deve-se considerar a estrutura da empresa, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados (art. 50º, parágrafo 1º e 2º, da Lei n. 13.709/2018).

A implementação dessas boas práticas é chamada na LGPD de programa de governança em privacidade, que, segundo o art. 50º, parágrafo 2º, deve conter, no mínimo:

> a) demonstração do comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento abrangente de normas e boas práticas relativas à proteção de dados pessoais;
>
> b) ser aplicável a todo o conjunto de dados pessoais sob seu controle, independentemente do modo como foram coletados;
>
> c) ser adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
>
> d) estabelecer políticas e salvaguardas adequadas com base em uma avaliação sistemática de impactos e riscos à privacidade;
>
> e) ter o objetivo de estabelecer uma relação de confiança com o titular, por meio de atuação transparente e assegurando mecanismos de participação do titular;
>
> f) estar integrado à estrutura geral de governança da empresa e estabelecer e aplicar mecanismos de supervisão internos e externos;
>
> g) contar com planos de resposta a incidentes e remediação; e

h) ser constantemente atualizado com base em informações obtidas através de monitoramento contínuo e avaliações periódicas.

Mesmo com a definição legal do que um programa de governança em privacidade deve considerar, é necessário que os controladores demonstrem a efetividade dessas práticas.

Os agentes de tratamento, por sua vez, devem adotar medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Além dos agentes, qualquer pessoa que intervenha em uma das fases do tratamento de dados está obrigada a garantir a segurança da informação em relação aos dados pessoais, mesmo após o seu término. Caso o controlador tome ciência da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, deverá comunicar à autoridade nacional e ao titular (art. 47º e 48º da Lei n. 13.709/2018).

Outro aspecto importante que deve ser considerado é que as regras de boas práticas e de governança devem ser publicadas e atualizadas periodicamente, podendo ser reconhecidas e divulgadas pela autoridade nacional.

TEMA 5 – AUDITORIA E PRIVACIDADE

Uma etapa importante para garantir a efetividade dos programas de governança em privacidade é a realização de auditorias periódicas, objetivando avaliar sua conformidade com as políticas e processos internos e com a LGPD.

Nesta etapa, devem ser realizadas avaliações de impacto à privacidade, especialmente em casos de tratamento de dados sensíveis ou de grande escala, atuando na identificação e mitigação de possíveis riscos à privacidade desde o início do processo de tratamento de dados.

As auditorias realizadas com essa finalidade envolvem a análise de políticas de privacidade, procedimentos de consentimento, medidas de segurança de dados, gestão de incidentes, além do cumprimento dos direitos dos titulares, como acesso, correção e exclusão de dados pessoais. Também consideram se as empresas estão implementando as salvaguardas necessárias

para proteger os dados contra acesso não autorizado, perda, roubo ou divulgação indevida.

Além de ser uma atividade necessária para garantir a conformidade legal, a auditoria também impacta na reputação da empresa junto aos seus stakeholders e na construção de relacionamentos mais sólidos, uma vez que demonstra seu compromisso com a proteção da privacidade e fortalece a confiança com todas as partes interessadas.

TROCANDO IDEIAS

"O Instituto Sigilo, com o apoio do Ministério Público Federal (MPF), abriu Ação Civil Pública contra a Serasa, na qual pede que a plataforma de proteção ao crédito seja condenada a pagar R$ 30 mil para cada indivíduo impactado pelo vazamento de dados em 2021 — a ocorrência afetou 223 milhões de pessoas." Fonte: <https://www.infomoney.com.br/minhas-financas/mpf-pede-que-serasa-pague-indenizacao-de-r-30-mil-para-cada-usuario-afetado-em-vazamento>. Acesso em: 26 jun. 2024.

Notícias como essa infelizmente ainda são comuns no Brasil. Muitos de nós já tivemos dados pessoais vazados indevidamente e, muitas vezes, não temos consciência disso. Compartilhe com seus colegas se você já foi alvo de vazamento de dados pessoais, como identificou esse fato e o procedimento adotado para se proteger.

NA PRÁTICA

(Enade 2021) Empreender em computação não se resume apenas ao fato de ter uma ideia sobre um aplicativo, implementá-la e disponibilizá-la aos seus usuários finais. Esse conceito vai além; é preciso analisar uma série de variáveis, como questões sociais, humanísticas, profissionais, ambientais, legais, políticas e tecnológicas.

Dentre as ações necessárias para empreender em computação, é imprescindível observar a legislação vigente. No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD), n. 13.709/2018, dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de

liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Acerca das providências dispostas no art. 2º da LGPD, assinale os fundamentos da disciplina da proteção de dados pessoais:

a) O direito ao usuário; às obrigações das organizações nacionais ou estrangeiras; à obrigatoriedade do consentimento; à livre iniciativa, à livre concorrência e à defesa do consumidor; aos direitos humanos, ao livre desenvolvimento da personalidade, à dignidade e ao exercício da cidadania pelas pessoas naturais; e à regulação da Autoridade Nacional de Proteção de Dados Pessoais (ANPD).
b) O direito à revogação do consentimento; à transferência de dados para outro fornecedor de serviços; à solicitação de remoção de dados pessoais; à inviolabilidade da intimidade, da honra e da imagem; ao desenvolvimento econômico e tecnológico, e à inovação; à preservação da vida e da integridade física das pessoas.
c) O respeito à privacidade; à obrigatoriedade do consentimento; aos deveres e obrigações dos usuários finais; aos deveres e obrigações das organizações nacionais ou estrangeiras; à observância ao código de defesa do consumidor; e à obrigatoriedade de respeitar à honra e à imagem.
d) O direito ao anonimato; à liberdade de expressão; à inviolabilidade da intimidade; à adoção de medidas preventivas de segurança; ao direito ao recurso e à revisão; à administração de riscos e falhas; ao estabelecimento de agentes de tratamento; e à regulação da Autoridade Nacional de Proteção de Dados Pessoais (ANPD).
e) O respeito à privacidade; à autodeterminação informativa; à liberdade de expressão, de informação, de comunicação e de opinião; à inviolabilidade da intimidade, da honra e da imagem; ao desenvolvimento econômico e tecnológico e à inovação; à livre iniciativa, à livre concorrência e à defesa do consumidor; e aos direitos humanos, ao livre desenvolvimento da personalidade, à dignidade e ao exercício da cidadania pelas pessoas naturais.

A resposta está na seção Gabarito, após as Referências.

FINALIZANDO

O cumprimento da Lei Geral de Proteção de Dados (LGPD) por parte das empresas é fundamental não apenas para garantir a segurança e privacidade dos dados dos clientes, mas também para fortalecer a confiança e a reputação da marca.

Ao adotar práticas de governança corporativa e compliance, as empresas podem garantir que os dados sejam coletados, armazenados e utilizados de acordo com as diretrizes estabelecidas pela legislação, minimizando riscos de vazamentos ou uso inadequado. Além disso, a implementação de medidas de governança e compliance não apenas demonstra o comprometimento da empresa com a proteção de dados, mas também contribui para a eficiência operacional e a sustentabilidade do negócio a longo prazo.

A governança corporativa e o compliance são pilares essenciais para o cumprimento da LGPD, pois fornecem estruturas e processos robustos para garantir a conformidade contínua com as regulamentações de proteção de dados.

REFERÊNCIAS

BRASIL. **Decreto n. 11.129, de 11 de julho de 2022**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/decreto/d11129.htm>. Acesso em: 26 jun. 2024.

_____. **Guia de boas práticas – Lei Geral de Proteção de Dados (LGPD)**. Brasília: Advocacia Geral da União, 2020. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf>. Acesso em: 26 jun. 2024.

_____. **Lei n. 12.846, de 1º de agosto de 2013**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm>. Acesso em: 26 jun. 2024.

CARVALHO, A. C.; BERTOCCELLI, R. de P.; ALVIM, T. C. et al. **Manual de Compliance**. Grupo GEN, 2021.

CGU – Controladoria Geral da União. **Lei Anticorrupção completa 10 anos de vigência**. 2024. Disponível em: <https://www.gov.br/cgu/pt-br/assuntos/noticias/2024/01/lei-anticorrupcao-completa-10-anos-de-vigencia. Acesso em: 26 jun. 2024.

COSO. **The Committee of Sponsoring Organizations of the Treadway** Commission. 2013. Disponível em: <https://www.coso.org/guidance-on-ic. Acesso em: 20 jun. 2024.

DA SILVA, H. J. Compliance e Integridade Empresarial: a valoração ética na governança corporativa. **Meritum**, Revista de Direito da Universidade FUMEC, 2022.

DELOITTE. **Integridade Corporativa no Brasil 2022 – Evolução do compliance e das boas práticas empresariais**. Disponível em: <https://www2.deloitte.com/br/pt/pages/risk/articles/integridade-corporativa-evolucao-do-compliance.html>. Acesso em: 26 jun. 2024.

EY – Ernest Young. **Relatório Global de Integridade EY 2022**. Disponível em: <https://www.ey.com/pt_br/forensic-integrity-services/how-a-focus-on-governance-can-help-reimagine-corporate-integrity>. Acesso em: 26 jun. 2024.

GARCIA, L. R. **Lei Geral de Proteção de Dados (LGPD)**: Guia de implantação. Blucher, 2020.

GET PRIVACY. **Tratamento de dados**: o que é e como ele é regulamentado pela LGPD. Disponível em: <https://getprivacy.com.br/tratamento-de-dados-lgpd>. Acesso em: 26 jun. 2024.

IBGC – Instituto Brasileiro de Governança Corporativa. **Código das melhores práticas de governança corporativa**. 5. ed. São Paulo: IBGC, 2015.

_____. **Código das melhores práticas de governança corporativa**. 6. ed. São Paulo: IBGC, 2023.

_____. **Governança Corporativa e Integridade Empresarial**. 1. ed. Saint Paul Publishing, 2017.

JENSEN, M. C.; ERHARD, W. Beyond Agency Theory: The Hidden and Heretofore Inaccessible Power of Integrity. **Harvard Business School Working Paper**, n. 10-068, Feb. 2010. Disponível em: <https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=1552009>. Acesso em: 3 ago. 2017.

JUNIOR, A. B.; GIACOMINI FILHO, G. Greenwashing e as organizações no contexto do século XXI. **Revista Metropolitana de Sustentabilidade**, v. 4, n. 1, p. 95-106, 2014.

OLIVEIRA, J. C. M. de. **Gestão de Riscos como ferramenta para a promoção da integridade pública**: um estudo com comissões de ética do Poder Executivo Federal. 2018.

ONU – Organização das Nações Unidas. **Objetivos de Desenvolvimento Sustentável**. Disponível em: <https://brasil.un.org/pt-br/sdgs>. Acesso em: 26 jun. 2024.

_____. **Pacto Global Nações Unidas**. Disponível em: <https://www.pactoglobal.org.br/sobre-nos/>. Acesso em: 26 jun. 2024.

ROSSETTI, J. P.; ANDRADE, A. **Governança corporativa**: fundamentos, desenvolvimento e tendências. 7. ed. Grupo GEN, 2014.

SILVA, E. C. da. **Governança Corporativa nas Empresas**. 4. ed. Grupo GEN, 2016.

SILVEIRA, R. de M. J.; SAAD-DINIZ, E. **Compliance, direito penal e lei anticorrupção**. São Paulo: Saraiva, 2015.

THE GLOGAL COMPACT. **Who Cares Wins**: Connecting Financial Markets to a Changing World. Disponível em: <https://www.unepfi.org/fileadmin/events/2004/stocks/who_cares_wins_global_compact_2004.pdf>. Acesso em: 26 jun. 2024.

TJSP – Tribunal de Justiça de São Paulo. **Lei Geral de Proteção de Dados**. Disponível em: < https://www.tjsp.jus.br/LGPD/LGPD/ALGPD>. Acesso em: 26 jun. 2024.

TRENNEPOHL, T.; TRENNEPOHL, N. **ESG e Compliance**: interfaces, desafios e oportunidades. Saraiva, 2023.

VALLE, P. **Depois do "greenwashing", cuidado com o "al whashing"**. O alerta é da SEC. Neofeed: 2023. Disponível em: <https://neofeed.com.br/wealth-management/depois-do-greenwashing-cuidado-com-o-ai-washing-o-alerta-e-da-sec>. Acesso em: 26 jun. 2024.

VIEIRA, J. B.; BARRETO, R. T. de S. **Governança, gestão de riscos e integridade**. 2019.

WILLIAMSON, O. **The Mechanisms of Governance**. New York: Oxford University Press, 1996.

GABARITO

Resposta: e)