DADOS EM PAUTA: A ADEQUAÇÃO DOS TRIBUNAIS DE JUSTIÇA À LGPD

Mariana Keppen

Presidente da Comissão de Compliance e Anticorrupção Empresarial da OAB/PR, diretora de compliance e proteção de dados do escritório Pironti Advogados e mestranda em Direito e Economia da Faculdade de Direito da Universidade de Lisboa.

RESUMO

A Lei Geral de Proteção de Dados (LGPD) trouxe desafios significativos ao estabelecer novos parâmetros para a atividade de tratamento de dados. Considerando a sua aplicação à administração pública, o Conselho Nacional de Justiça (CNJ) publicou a Resolução nº 363/2021, que visa a orientar os tribunais na implementação da LGPD. Este artigo explora a importância da conformidade com a LGPD nos Tribunais de Justiça, enfatizando a necessidade de análise e dedicação específicas, bem como aborda metodologia para atender aos requisitos de proteção de dados nesse contexto.

Palavras-chave: Privacidade. Proteção de dados. Poder Judiciário. Metodologia.

ABSTRACT

The Brazilian General Data Protection Law (LGPD) has brought significant challenges by establishing new parameters for data processing activities. Considering its application to the public administration, the National Council of Justice (CNJ) has published Resolution 363/2021, aimed at guiding the courts in implementing the LGPD. This article explores the importance of LGPD compliance in the Courts of Justice, emphasizing the need for specific analysis and dedication, as well as addressing the methodology to meet data protection requirements in this context.

Keywords: Privacy. Data protection. Judiciary. Methodology.

1. INTRODUÇÃO

A Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018), mais conhecida como LGPD, entrou em vigor em setembro de 2020 e inaugurou um novo paradigma em relação à privacidade e proteção de dados no Brasil. Seguindo a tendência da União Europeia, que desde 2016 tem o Regulamento Geral de Proteção de Dados Pessoais (GDPR), as instituições públicas e privadas que realizem tratamento de dados pessoais precisam estar adequadas às suas previsões.

Se o desafio já é bastante grande para os atores privados, quando falamos do âmbito público esse desafio se torna ainda maior. Devido às especificidades do Poder Judiciário, são necessários cautela e estudo dedicado na condução das adequações à LGPD nessa esfera. É certo que muitas medidas implementadas por pessoas jurídicas de direito privado também se aplicam às públicas. Como exemplo, citamos a necessidade da realização de um mapeamento de dados (muitas vezes referido por seu nome em inglês, *data mapping*) e a elaboração de uma matriz de riscos que contemple todos os tratamentos de dados realizados e os riscos relacionados a eles.

Entretanto, o debate específico em relação à aplicação da Lei Geral de Proteção de Dados no âmbito do Poder Judiciário e Tribunais de Justiça é de extrema importância e merece dedicação em sua análise. Nesse sentido, o CNJ publicou em janeiro de 2021 a Resolução nº 363, que estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais (LGPD) a serem adotadas pelos tribunais do país (primeira e segunda instâncias e cortes superiores), à exceção do Supremo Tribunal Federal, com o objetivo de facilitar o processo de implementação da legislação de proteção de dados no âmbito do sistema judicial.

Este artigo, portanto, se dedica a explanar sobre alguns aspectos da condução do processo de adequação à Lei Geral de Proteção de Dados no contexto de Tribunais de Justiça.

2. ESTABELECIMENTO DE UMA METODOLOGIA DE ADEQUAÇÃO

Da leitura da Resolução nº 363/2021, percebe-se que o CNJ busca incentivar não somente a adequação dos tribunais à LGPD, mas a implementação de um Programa de Governança de Dados, conforme referido na lei, ou também conhecido como Sistema de Privacidade e Proteção de Dados. Isso porque a resolução, mais do que a conformidade com a lei, busca estimular as melhores práticas relacionadas à proteção de dados e, principalmente, fortalecer a cultura de privacidade no âmbito do sistema judicial.

Esse objetivo fica evidente nas orientações relacionadas à criação de um Comitê Gestor de Proteção de Dados Pessoais (CGPD), que será o responsável pelo processo de implementação da Lei nº 13.709/2018 em cada tribunal (art. 1º, I), e à organização de um programa de conscientização sobre a LGPD, destinado a magistrados, servidores, trabalhadores terceirizados, estagiários e residentes judiciais (art. 1º, IX).

Ainda, a Resolução nº 363/2021estabelece a realização do mapeamento de todas as atividades de tratamento de dados pessoais, a avaliação de riscos (*gap assessment*) e o estabelecimento de planos de ação (*roadmap*) para atendimento da LGPD e resolução (art. 2º, I, II e III). Nesse sentido, visando ao atendimento às normativas de proteção de dados e à garantia da privacidade, é necessário desenvolver um projeto que viabilize a condução e gestão das atividades a serem realizadas, considerando a dimensão de atuação dos Tribunais de Justiça e o volume de tratamentos de dados realizados.

Para tanto, será apresentada no presente artigo uma sugestão de metodologia para o desenvolvimento das atividades de adequação e atendimento à Resolução nº 363/2021 do CNJ e implementação de um Sistema de Privacidade e Proteção de Dados. Com efeito, essa metodologia foi desenhada com base em diretrizes nacionais e internacionais sobre o tema, como as normas ISO 31000:2018, 27001:2013, 27002:2022 e 27701:2019, metodologia COSO e diretrizes do Instituto de Auditores Internos - IIA, com especial destaque às orientações divulgadas

pela Autoridade Nacional de Proteção de Dados (ANPD)[1]. Esquematicamente, a metodologia pode ser traduzida na ilustração a seguir:

Conforme apresentado, as atividades de adequação estão divididas em 10 módulos temáticos, desenvolvidos com base

1 Metodologia desenvolvida e aplicada pelo escritório Pironti Advogados, sendo a autora a diretora de Compliance e Proteção de Dados.

no cenário de riscos identificado no Módulo I. Nessa metodologia, o Módulo X, notadamente, relacionado ao Treinamento e Comunicação, atravessa todos os outros módulos, devido à sua significativa importância na promoção do engajamento dos servidores e magistrados envolvidos no projeto. Além disso, este desempenha um papel fundamental na consolidação da cultura de privacidade e proteção de dados dentro da instituição, bem como na melhoria da transparência em relação às atividades de tratamento de dados pessoais realizadas.

Para uma melhor análise em relação às previsões da Resolução nº 363/2021 do CNJ, os módulos serão abordados individualmente a seguir.

2.1. Módulo I - Data Mapping & Risk Assessment

Dentro do conjunto de iniciativas que compõem a metodologia apresentada, destaca-se o primeiro módulo (Data Mapping & Risk Assessment) como uma etapa fundamental para o processo de adequação à LGPD. Isso ocorre porque o Módulo I desempenha um papel central na compreensão dos tratamentos de dados pessoais realizados e na avaliação dos riscos associados a eles. Portanto, serve como a base lógica para todas as demais ações a serem desenvolvidas.

O mapeamento de dados, também conhecido como inventário de dados, é uma etapa necessária para a conformidade com a Lei Geral de Proteção de Dados, e deve ser o ponto de partida para todas as medidas a serem adotadas para atingir esse objetivo. Notadamente, o artigo 37 da LGPD estabelece a obrigação do controlador de dados de manter registros das operações de tratamento que realiza. Já a Resolução nº 363/2021 do CNJ traz previsão semelhante em seu artigo 1º, XII, sendo o mapeamento de dados a consolidação dessa exigência.

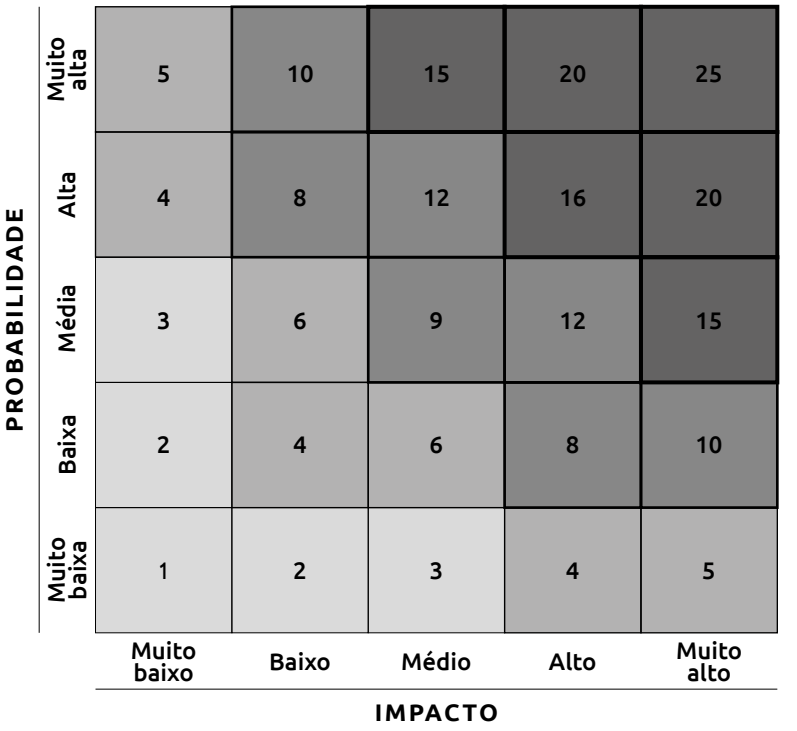
De forma mais específica, a Resolução elenca que devem ser registradas, ao menos, as seguintes informações: a) finalidade do tratamento; b) base legal; c) descrição dos titulares; d) categorias de dados; e) categorias de destinatários; f) eventual transferência internacional; e g) prazo de conservação e medi-

das de segurança adotadas.

A partir da consolidação do mapeamento de dados, torna-se possível desenvolver a Matriz de Riscos e os Relatórios de Impacto à Proteção de Dados (RIPD). A avaliação de riscos, que é precedida pelo mapeamento dos processos, ativos e terceiros envolvidos nas atividades de tratamento de dados realizadas pelo Tribunal, é a base das medidas a serem adotadas para aprimorar a privacidade e a proteção de dados dentro da instituição. Isso é de extrema importância para a conformidade com a LGPD, já que a própria lei, no § 1º do artigo 50, exige que os agentes considerem a natureza, o escopo, a finalidade, a probabilidade e a gravidade dos riscos e benefícios decorrentes do tratamento de dados do titular ao definirem medidas organizacionais. Além disso, a partir do mapeamento de dados e da avaliação de riscos, é possível mensurar o grau de risco e o impacto dos tratamentos aos direitos dos titulares, permitindo a definição dos tratamentos que serão objeto de Relatório de Impacto à Proteção de Dados (RIPD).

A elaboração de tais relatórios é fundamental para o gerenciamento dos riscos associados ao tratamento de dados pessoais que possam afetar as liberdades civis e os direitos fundamentais, conforme definido no artigo 5º, XVII, da Lei nº 13.709/2018, e para o processo de documentação e gestão dos registros e informações que o controlador deve manter para monitorar seu processo de tratamento de dados, bem como estabelecer medidas, salvaguardas e mecanismos de mitigação de riscos.

Em resumo, a elaboração do Data Mapping & Risk Assessment (Módulo I) serve como o ponto de partida para a conformidade com a LGPD, pois seu conteúdo é essencial para entender o cenário de risco, representado no Mapa de Calor 5x5 (conforme imagem abaixo) e determinar as medidas necessárias (planos de ação) e que serão implementadas ao longo do projeto de adequação à LGPD.



Importante ressaltar que essa é exatamente a lógica proposta pela Resolução nº 363/2021 do CNJ, que prevê em seu artigo 2º a seguinte cadência:

> I - realização do mapeamento de todas as atividades de tratamento de dados pessoais por meio de questionário, conforme modelo a ser elaborado pelo CNJ;
>
> II - realização da avaliação das vulnerabilidades (*gap assessment*) para a análise das lacunas da instituição em relação à proteção de dados pessoais; e
>
> III - elaboração de plano de ação (*roadmap*), com a previsão de todas as atividades constantes nesta Resolução.

2.2. Módulo II - Estrutura Organizacional

Passando aos módulos que concretizam os planos de ação previstos na etapa de diagnóstico, o primeiro deles diz respeito à estrutura organizacional de proteção de dados, que é composta pelo encarregado de dados, também conhecido como Data Protection Officer (DPO), e pelo Comitê Gestor de Proteção de Dados Pessoais (CGPD).

O encarregado de dados desempenha um papel de relevância ao facilitar a comunicação entre os responsáveis pelo tratamento de dados, os titulares dos dados e a Autoridade Nacional de Proteção de Dados. Nesse contexto, suas responsabilidades incluem receber e responder às solicitações dos titulares, fornecendo esclarecimentos apropriados; gerenciar as comunicações recebidas da Autoridade Nacional de Proteção de Dados, tomando as medidas necessárias em conformidade com a legislação; além de orientar os colaboradores sobre as melhores práticas relacionadas à proteção de dados pessoais.

A nomeação do encarregado de dados está prevista no artigo 41 da LGPD, bem como no artigo 1º, II, da Resolução nº 363/2021 do CNJ. Entretanto, essa resolução, para além do encarregado, estabelece a necessidade de implantação de um Comitê Gestor de Proteção de Dados Pessoais, conforme a sequência do artigo 1º:

> I - criar o Comitê Gestor de Proteção de Dados Pessoais (CGPD), que será o responsável pelo processo de implementação da Lei nº 13.709/2018 em cada tribunal, com as seguintes características:
>
> a) a composição do referido Comitê deverá ter caráter multidisciplinar e ter em vista o porte de cada tribunal;
>
> b) caberá a cada tribunal a decisão de promover a capacitação dos membros do CGPD sobre a LGPD e normas afins, o que poderá ser viabilizado pelas academias ou escolas judiciais das respectivas Cortes de Justiça.

Sendo assim, adicionalmente, no âmbito dos Tribunais de Justiça, a estrutura organizacional será complementada pela formação do Comitê Gestor de Proteção de Dados Pessoais, que terá como função principal a tomada de decisões estraté-

gicas relacionadas ao sistema e a supervisão das atividades desempenhadas pelo encarregado de dados.

Destaca-se, por fim, que essa estrutura desempenha um papel fundamental no efetivo gerenciamento de riscos associados à privacidade e proteção de dados. Nesse sentido, importante que seus membros sejam capacitados e recebam o apoio necessário para a condução de suas atividades.

2.3. Módulo III - Políticas de Privacidade e Proteção de Dados

A revisão, elaboração e implementação de políticas comportamentais e procedimentais relacionadas ao Sistema de Privacidade e Proteção de Dados, considerando as priorizações em relação aos níveis de risco identificados e as necessidades do Tribunal, desempenham uma função de extrema relevância no processo de conformidade com a Lei Geral de Proteção de Dados (LGPD).

Essas políticas têm um impacto fundamental ao formalizar as novas diretrizes e normas a serem seguidas, demonstrando de maneira clara e precisa o compromisso da instituição com a privacidade e proteção de dados pessoais. Além disso, promovem a transparência sobre a maneira como os dados são tratados durante a execução das atividades institucionais. Importante observar que essas políticas sejam elaboradas tendo em consideração a realidade específica da instituição e conforme o cenário de riscos identificado durante a fase de diagnóstico do projeto.

De um modo geral, deve ser elaborada a Política de Privacidade, que contenha ao menos as finalidades dos principais tratamentos, as hipóteses legais que baseiam tais tratamentos, a forma como os titulares poderão exercer seus direitos, o contato do encarregado de dados e as medidas e salvaguardas utilizadas pela instituição para garantir a privacidade e proteção de dados.

Ainda, sugere-se que seja revisada a Política de Segurança da Informação do Tribunal, com o objetivo de que seja validada sua adequação às previsões da LGPD.

2.4. Módulo IV - Resposta a Incidentes de Segurança

O tratamento de dados pessoais realizado pelo Tribunal expõe, invariavelmente, a instituição a riscos inerentes a essas atividades, ainda que todas as medidas de prevenção e mitigação sejam adotadas. É essencial, portanto, que as equipes dos Tribunais de Justiça estejam preparadas e saibam como atuar caso riscos venham a se concretizar, razão pela qual o Sistema de Privacidade e Proteção de Dados também contempla, em seu Módulo IV, o desenvolvimento de um Plano de Resposta a Incidentes de Segurança envolvendo dados pessoais.

O estabelecimento de um Plano de Resposta a Incidentes atende à previsão das Boas Práticas de Governança do artigo 50 da LGPD, e permite que o Tribunal apresente respostas mais eficientes diante dos incidentes, viabilizando a análise e, quando necessária, a comunicação de incidentes aos titulares de dados e à Autoridade Nacional de Proteção de Dados.

2.5. Módulo V - Gestão de Terceiros

A Lei Geral de Proteção de Dados inova ao estabelecer uma cadeia de responsabilidade relacionada ao tratamento de dados, representada pelos agentes de tratamento (controladores e operadores). Sendo assim, no escopo de adequação à LGPD, é necessário diagnosticar a definição dos papéis no relacionamento com terceiros que realizem tratamento de dados pessoais, de modo que as cláusulas contratuais que regem tais relações estejam adequadas às responsabilidades e apropriadas à mitigação de riscos. Devem ser revisitados, portanto, os modelos de contratos de fornecedores, convênios, parcerias e, inclusive, de trabalho. No mesmo sentido, o artigo 1º da Resolução nº 363/2021 do CNJ estabelece como medida necessária:

> X - revisar os modelos de minutas de contratos e convênios com terceiros já existentes, que autorizem o compartilhamento de dados, bem como elaborar orientações para as contratações futuras, em conformidade com a LGPD, considerando os seguintes critérios:

a) para uma determinada operação de tratamento de dados pessoais deve haver:

1. uma respectiva finalidade específica;

2. em consonância ao interesse público; e

3. com lastro em regra de competência administrativa aplicável à situação concreta.

b) o tratamento de dados pessoais previsto no respectivo ato deve ser:

1. compatível com a finalidade especificada; e

2. necessário para a sua realização.

c) inclusão de cláusulas de eliminação de dados pessoais nos contratos, convênios e instrumentos congêneres, à luz dos parâmetros da finalidade e da necessidade acima indicados.

Da mesma forma, é essencial que o Tribunal verifique o nível de adequação de seus fornecedores e terceiros em relação à Lei Geral de Proteção de Dados Pessoais, através, por exemplo, da aplicação de diagnóstico de adequação dos terceiros com os quais se relaciona, com o objetivo de formalizar a diligência da instituição e estabelecer um canal de comunicação e mútua contribuição em relação aos agentes de tratamento que integram sua cadeia de tratamento de dados pessoais.

2.6. Módulo VI - Direitos dos Titulares

Além da diligência em relação aos terceiros, a LGPD também exige um olhar atento ao titular dos dados pessoais, pois tem como um de seus princípios a autodeterminação informativa, a qual garante ao titular o controle de como e para quais finalidades os seus dados serão utilizados.

Sendo assim, no projeto de adequação à LGPD, deverão ser adotadas medidas para viabilizar que os titulares de dados pessoais possam exercer o rol de direitos estabelecido nos artigos 17, 18 e 20[2] da legislação de proteção de dados. Para tanto, a

2 Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

Resolução nº 363/2021 do CNJ estabelece (artigo 1º) que o Tribunal deverá:

> IV - elaborar, por meio de canal do próprio encarregado, ou em parceria com as respectivas ouvidorias dos tribunais:
>
> a) formulário eletrônico ou sistema para atendimento das requisições e/ou reclamações apresentadas por parte dos titulares dos dados pessoais;
>
> b) fluxo para atendimento aos direitos dos titulares (art. 18, 19 e 20 da LGPD), requisições e/ou reclamações apresentadas, desde o seu ingresso até o fornecimento da respectiva resposta.

Nesse sentido, o Tribunal de Justiça deverá estabelecer um Sistema de Privacidade e Proteção de Dados que contemple fluxos de resposta aos titulares e protocolos para acompanhar e atender às solicitações de forma eficaz, permitindo que os titulares exerçam seus direitos de maneira simplificada.

Adicionalmente, orienta-se que seja elaborado um Guia de Direitos dos Titulares, com o objetivo de proporcionar transparência aos titulares sobre como exercer tais direitos. É relevante ressaltar que todas as solicitações deverão ser avaliadas à luz da Lei Geral de Proteção de Dados Pessoais, e, mesmo que uma solicitação não seja considerada procedente, é importante que

---

Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: I - confirmação da existência de tratamento; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

seja dada uma negativa fundamentada ao titular de dados, explicando as razões pelas quais o pedido não pôde ser atendido.

Além disso, o fluxo de atendimento dos titulares contemplará as situações em que o Comitê Gestor de Proteção de Dados Pessoais será envolvido no processo de análise das solicitações, de modo a estabelecer um tratamento adequado e transparente das demandas relacionadas à privacidade dos titulares de dados.

2.7. Módulo VII - Sistema de Segurança da Informação

Ao abordar a Lei Geral de Proteção de Dados Pessoais, é fundamental manter em mente o aspecto técnico de segurança da informação que está intrinsicamente relacionado a essa legislação. Apesar de serem conceitos distintos – a segurança da informação vai além dos dados pessoais e diz respeito a todos os dados e informações que uma instituição trata no decorrer de suas atividades – ambos estão diretamente relacionados, uma vez que o sistema de segurança da informação se preocupa com o conjunto de mecanismos e controles ligados à tecnologia da informação que visam a proteger e resguardar todos os tipos de dados – e entre esses se incluem os pessoais.

Nesse sentido, é crucial considerar a implementação de um Sistema de Segurança da Informação, composto por uma série de mecanismos e controles relacionados à tecnologia da informação. Esse sistema tem como propósito a proteção e a preservação das informações, através, por exemplo, da avaliação de *firewalls*, implementação de medidas de segurança contra *ransomware*, simulação de ataques de *phishing* para avaliar o grau de conscientização das pessoas na instituição em relação a essa ameaça e análise de vulnerabilidades externas em sistemas com acesso externo que contenham dados pessoais.

Essas medidas técnicas estão previstas no inciso XI do artigo 1º da Resolução nº 363/2021 do CNJ, e contribuirão para a conformidade completa com a LGPD, garantindo a proteção eficaz dos dados pessoais e de todas as informações tratadas pela instituição.

2.8. Módulo VIII - Sistema de Transparência

A implementação da Lei Geral de Proteção de Dados em instituições públicas levanta a discussão relacionada à compatibilização das previsões da LGPD com as diretrizes de transparência impostas pela Lei de Acesso à Informação. Nesse sentido, é importante que seja realizada uma análise das iniciativas de transparência do Tribunal no sentido de garantir a conciliação destas com a privacidade e proteção de dados.

Para tanto, sugere-se a análise crítica do Portal da Transparência da instituição e a elaboração de fluxo de recebimento de solicitações relacionadas à transparência que envolvam dados pessoais, de modo que o encarregado de dados e o Comitê Gestor de Proteção de Dados Pessoais sejam envolvidos, quando necessário.

2.9. Módulo IX - Redesenho de Processos

Por sua vez, o módulo referente ao Redesenho de Processos é de suma importância, porque demonstra que a instituição prioriza uma atitude proativa, e não reativa no que diz respeito ao tratamento de dados e proteção da privacidade. Sendo assim, o desenho de processos ou o redesenho, quando necessário, são fundamentais para a efetividade do Sistema de Privacidade de Dados da instituição, e contempla a análise crítica dos processos existentes, com o objetivo de identificação de oportunidades de melhoria e, se necessário, a implementação de novos processos, sempre com foco na proteção da privacidade. A título de exemplo, usualmente são objeto de revisão os processos relacionados à gestão de pessoas, contratação de terceiros, controle de acessos e compartilhamento de dados.

2.10. Módulo X - Treinamento e Comunicação

O propósito final do processo de implantação de um sistema de privacidade e de adequação à Lei Geral de Proteção de

Dados é o estabelecimento de uma cultura organizacional voltada à proteção e ao respeito ao tratamento de dados de pessoas naturais. Esse aculturamento pressupõe a realização periódica de uma série de treinamentos e comunicações com a finalidade de promover a privacidade e a proteção de dados, uma vez que é somente através do constante treinamento e orientação que todos os demais módulos do sistema de privacidade serão verdadeiramente incorporados ao dia a dia da Instituição.

Nesse sentido, a Resolução nº 363/2021 do CNJ, em seu artigo 1º, IX, estabelece a previsão de que seja organizado um programa de conscientização sobre a LGPD, destinado a magistrados, servidores, trabalhadores terceirizados, estagiários e residentes judiciais, das áreas administrativas e judiciais de primeira e de segunda instâncias.

Para além dos treinamentos, recomenda-se que sejam utilizadas estratégias de comunicação, a exemplo da publicação de pílulas de LGPD, para que seja mantido em pauta o tema da proteção de dados e externado o compromisso da instituição com a privacidade e proteção de dados.

3. CONCLUSÃO

A Lei Geral de Proteção de Dados Pessoais (LGPD) estabeleceu um conjunto de obrigações que precisam ser observadas, inclusive no âmbito da administração pública, como é o caso dos Tribunais de Justiça. Nesse sentido, a implementação de Sistemas de Privacidade e Proteção de Dados nas instituições do Poder Judiciário tem como finalidade não apenas cumprir com as exigências legais de proteção de dados, mas também desempenhar seu o papel fundamental na consolidação dos direitos individuais e na promoção da cultura de privacidade.

No presente artigo, buscou-se apresentar uma possibilidade de metodologia a ser adotada e, sobretudo, contribuir para o debate acadêmico e prático sobre o tema. Nesse contexto, foram abordados os desafios e as melhores práticas relacionadas

à conformidade com a legislação de proteção de dados em instituições jurídicas, reconhecendo sua importância no contexto legal e, principalmente, social.

REFERÊNCIAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>.

CONSELHO NACIONAL DE JUSTIÇA. Resolução nº 363, de 12 de janeiro de 2021 Disponível em: <original181204202101196007 20f42c02e.pdf (cnj.jus.br)>.