

UNIVERSIDADE REGIONAL INTEGRADA DO ALTO URUGUAI E DAS MISSÕES
PRÓ-REITORIA DE ENSINO, PESQUISA E PÓS-GRADUAÇÃO
CAMPUS DE ERECHIM
DEPARTAMENTO DE CIÊNCIAS SOCIAIS APLICADAS
CURSO DE DIREITO

EDUARDO COGHETTO

**OS DESAFIOS DOS CARTÓRIOS DE REGISTROS CIVIS PARA SE ADAPTAREM
AOS PRECEITOS ARRAZOADOS PELA PROMULGAÇÃO DA LEI Nº 13.709/2018**

ERECHIM

2023

EDUARDO COGHETTO

**OS DESAFIOS DOS CARTÓRIOS DE REGISTROS CIVIS PARA SE ADAPTAREM
AOS PRECEITOS ARRAZOADOS PELA PROMULGAÇÃO DA LEI Nº 13.709/2018**

Trabalho apresentado ao Curso de Direito do Departamento de Ciências Sociais Aplicadas da Universidade Regional Integrada do Alto Uruguai e das Missões (URI) – Erechim/RS, como requisito parcial para obtenção do título de Bacharel em Direito.

Orientador(a): Prof. Dra. Giana Lisa Zanardo Sartori

ERECHIM

2023

EDUARDO COGHETTO

**OS DESAFIOS DOS CARTÓRIOS DE REGISTROS CIVIS PARA SE ADAPTAREM
AOS PRECEITOS ARRAZOADOS PELA PROMULGAÇÃO DA LEI Nº 13.709/2018**

Trabalho de conclusão de curso apresentado como requisito parcial para obtenção do título de Bacharel em Direito, pelo Curso de Direito do Departamento de Ciências Sociais Aplicadas da Universidade Regional Integrada do Alto Uruguai e das Missões.

Erechim/RS, 08 de novembro de 2023.

BANCA EXAMINADORA

Giana Lisa Zanardo Sartori, Professora Doutora, URI Erechim-RS.

(Luiz Mario Silveira Spinelli, Professor Mestre, URI Erechim-RS).

(Rafael Sottili Testa, Professor Doutor, URI Erechim-RS).

Dedico primeiramente a Deus, que foi quem mais me escutou nas horas que precisei. Também dedico aos meus pais, que foram eles a base de toda essa trajetória, desde o início até agora.

AGRADECIMENTOS

A minha instituição que nunca fez faltar nada. Foi sempre solícita e preocupada com o acadêmico.

A Prof. Dra. Giana Lisa Zanardo Sartori, pela excelente orientação, com seu gigantesco conhecimento acerca dos fatos, sempre se mostrou preocupada com o andamento deste, e sempre estava disposta a ajudar e responder aos questionamentos sempre que indagada. Não há palavras suficientes para descrever o quão satisfeito fiquei com o aceite de ser minha orientanda.

A alguns colegas de turma, que sempre estavam dispostos a ajudar, que enfrentamos os desafios juntos e chegamos ao mesmo objetivo, a conclusão do curso.

Aos amigos e familiares que muito escutaram reclamar sobre a faculdade, mas sempre munidos de palavras de conforto e incentivo, nunca deixaram pensar no pior.

A Deus, novamente, por ter sido o caminho da luz para a conclusão do curso.

“Por isso não tema, pois estou com você; não tenha medo, pois sou o seu Deus. Eu o fortalecerei e o ajudarei; Eu o segurarei com a minha mão direita vitoriosa.”

Isaías 41:10

Bíblia Sagrada

RESUMO

A pessoa natural é o indivíduo humano considerado sujeito de direitos e deveres perante a lei, possuindo identidade e personalidade jurídica. No entanto, à medida que a sociedade evolui, todos ficam vulneráveis aos males existentes, incluindo ameaças à privacidade e segurança dos dados pessoais. Nesse contexto, foi promulgada a Lei 13.709/2018, mais conhecida como Lei Geral de Proteção de Dados (LGPD), que compreende 65 artigos e estabelece diretrizes e regras para o tratamento de dados pessoais. A LGPD surgiu para proteger os indivíduos e seus dados em um cenário cada vez mais digital e interconectado. No entanto, dada a sua natureza recente, a aplicação dessa legislação apresenta desafios significativos para os Cartórios de Registro Civil, instituições que desempenham um papel fundamental na documentação e identificação dos cidadãos, diante disso os objetivos deste estudo incluem investigar como os cartórios de registro civil estão se adaptando à LGPD, identificar as principais questões e desafios enfrentados e propor estratégias para garantir a conformidade e a proteção efetiva dos dados pessoais dos cidadãos. Para isso, é necessário adotar na metodologia de pesquisa o método indutivo e o analítico-descritivo, a fim de examinar os desafios que os Cartórios de Registro Civil enfrentarão ao se adaptarem a essa nova realidade e a técnica de pesquisa bibliográfica e documental. Os Registros Cíveis coletam uma quantidade considerável de informações sensíveis, como nomes, datas de nascimento e números de identificação. Garantir que os cidadãos compreendam e concordem com o uso e tratamento de dados será crucial. Além disso, os Cartórios terão que investir em medidas de segurança da informação para proteger os dados pessoais sob sua responsabilidade. A LGPD exige a implementação de políticas e práticas que garantam a confidencialidade, integridade e disponibilidade dessas informações, evitando acessos não autorizados e vazamentos. Outro ponto de atenção está relacionado à transparência. Os Registros Cíveis devem informar claramente aos cidadãos como seus dados serão tratados, garantindo que eles tenham acesso a informações sobre o processo de coleta e uso de suas informações pessoais.

Palavras-chave: pessoa natural; Lei Geral de Proteção de Dados (LGPD); cartórios de registro civil; desafios; tratamento de dados

ABSTRACT

A natural person is a human individual considered subject to rights and duties before the law, having identity and legal personality. However, as society evolves, everyone becomes vulnerable to existing evils, including threats to privacy and personal data security. In this context, Law 13,709/2018, better known as the General Data Protection Law (LGPD), was enacted, which comprises 65 articles and establishes guidelines and rules for the processing of personal data. In an increasingly digital and interconnected scenario, LGPD emerged to protect individuals and their data. However, given its recent nature, the application of this legislation presents significant challenges for Civil Registry Offices, institutions that play a fundamental role in the documentation and identification of citizens. Understanding the precepts of the LGPD is essential to analyse the implications that this legislation will have for the services provided by Civil Registries. To achieve this, it is necessary to adopt analysis methods such as inductive and analytical-descriptive, in order to examine the challenges that Civil Registry Offices will face in adapting to this new reality. Civil Records collect a considerable amount of confidential information, such as names, dates of birth and identification numbers. It will be crucial to ensure that citizens understand and agree to the use and processing of data. Furthermore, Notaries will have to invest in information security measures to protect personal data under their responsibility. The LGPD requires the implementation of policies and practices that guarantee the confidentiality, integrity and availability of this information, preventing unauthorized access and leaks. Another point of attention is related to transparency. Civil Registries must clearly inform citizens about how their data will be treated, ensuring that they have access to information about the process of collecting and using their personal data.

Keywords: natural person; General Data Protection Law (LGPD); civil registry offices; challenges; Data processing

SUMÁRIO

1 INTRODUÇÃO.....	10
2 BREVES CONSIDERAÇÕES SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD).....	12
2.1 À LETRA DA LEI	12
2.2 AS SANÇÕES	20
2.3 A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E O CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE (CNPD)	21
3 ENQUADRAMENTO DA LGPD NOS CARTÓRIOS DE REGISTRO CIVIL	25
3.1 O QUE É O PESSOA NATURAL E O REGISTRO CIVIL DE PESSOAS NATURAIS	25
3.1.1 Do registro de nascimento	27
3.1.2 Do registro de casamento	28
3.1.3 Do registro de óbito	30
3.2 PROVIMENTOS REGULAMENTANDO O SERVIÇO ELETRÔNICO NOS CARTÓRIOS DE REGISTRO CIVIL	31
3.3 PROVIMENTO 134/2022 CNJ, A ADAPTAÇÃO DOS RCPN's À LGPD	34
4 OS DESAFIOS PARA OS RCPNs SE ADEQUAREM À LGPD.....	42
4.1 DO MAPEAMENTO DAS ATIVIDADES DE TRATAMENTO	44
4.2 DO DIAGNÓSTICO DE AÇÕES PRIORITÁRIAS.....	45
4.3 DA IMPLEMENTAÇÃO DE MEDIDAS NECESSÁRIAS.....	48
4.4 MEDIDAS DE SEGURANÇA E TREINAMENTO DE SEUS PREPOSTOS.....	50
4.5 DA TRANSPARÊNCIA.....	54
4.6 DA PUBLICIDADE DOS DADOS.....	55
5 CONCLUSÃO.....	60
REFERÊNCIAS.....	62

1 INTRODUÇÃO

A Lei Geral de Proteção de Dados (LGPD)¹ representa um marco fundamental na legislação brasileira, estabelecendo diretrizes e obrigações para a proteção de informações pessoais em um mundo cada vez mais digitalizado. Seu impacto abrange diversas áreas, e neste trabalho de conclusão de curso, o foco está na sua aplicação nos cartórios de registro civil, destacando a importância deste tema e as razões que motivaram a elaboração deste estudo.

A proteção de dados pessoais é uma preocupação global em um contexto onde informações sensíveis são constantemente compartilhadas e armazenadas. Nos cartórios de registro civil, a LGPD assume um papel crucial, uma vez que essas instituições lidam com uma vasta quantidade de dados pessoais, como certidões de nascimento, casamento e óbito. A natureza desses registros torna essencial garantir a conformidade com a legislação de proteção de dados para resguardar a privacidade e os direitos dos cidadãos.

A escolha deste tema se deve à sua relevância no cenário atual. A LGPD é uma lei recente, e os cartórios de registro civil estão enfrentando desafios únicos para se adaptar a esse novo quadro regulatório. Esta pesquisa busca justificar a importância de entender como essas instituições estão lidando com as implicações da LGPD, contribuindo assim para um conhecimento mais aprofundado sobre a conformidade legal e as melhores práticas nesse setor.

Esta pesquisa se concentra especificamente na aplicação da LGPD nos cartórios de registro civil, delimitando o escopo aos desafios e oportunidades enfrentados por essas instituições. No entanto, a proteção de dados pessoais é um tema amplamente discutido em diversos setores, e este estudo contribui ao fornecer percepções específicas para um campo de atuação essencial para a vida dos cidadãos.

Os objetivos deste estudo incluem investigar como os cartórios de registro civil estão se adaptando à LGPD, identificar as principais questões e desafios enfrentados e propor estratégias para garantir a conformidade e a proteção efetiva dos dados pessoais dos cidadãos.

¹ Será utilizada a forma abreviada da Lei Geral de Proteção de Dados (LGPD) durante todo o texto monográfico.

O trabalho está organizado da seguinte forma: no primeiro capítulo, será apresentada uma visão geral da LGPD e seu impacto geral; no segundo, pretende-se explorar a especificidade dos cartórios de registro civil e as implicações da LGPD neste contexto e no terceiro, serão analisados os desafios enfrentados pelos cartórios para garantir a conformidade com a LGPD. O método de pesquisa utilizado foi o indutivo, analítico descritivo, através da técnica de pesquisa bibliográfica e documental.

2 BREVES CONSIDERAÇÕES SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

2.1 À LETRA DA LEI

Com o transcurso do tempo, muitas coisas mudam e evoluem. Na sociedade, observa-se mudanças culturais, avanços tecnológicos e mudanças políticas. O passar do tempo traz mudanças inevitáveis, e é importante estar disposto a se adaptar e evoluir para acompanhar essas mudanças. Isso nos permite crescer e nos tornar melhores ao longo do tempo.

A forma como as pessoas vivem, trabalham e se comunicam tem sido transformada pela era digital. Para Rodolfo (2023), estaria passando pela Terceira Revolução Industrial, ou seja, é um ciclo de renovação de ideias, ações e pensamentos que marcaram a história da sociedade. Ainda comenta que, por exemplo, a era digital emerge como uma substituição à era industrial que, por sua vez, emergiu outrora em substituição à era da agricultura.

Com o exponencial avanço tecnológico, ficamos cada vez mais dependentes dessas novas tecnologias, como por exemplo smartphones, computadores, internet, entre outros, que, por um lado, simplificam e ajudam todos no dia-a-dia, porém, tornam todos dependentes de certas funcionalidades. Isso abre brechas para novas ondas de crimes cibernéticos, golpes, dentre outras injustiças. E em um mundo cada vez mais informatizado, novas “minas de ouro” surgem, nesse caso, os dados pessoais.

A proteção de dados pessoais é um assunto de extrema importância nos dias de hoje, especialmente com o crescente uso de tecnologias e da internet em nossas vidas. A proteção de dados pessoais se refere a garantir que as informações pessoais de uma pessoa sejam tratadas com segurança, privacidade e de acordo com a lei.

Nesse sentido, no dia 14 de agosto de 2018, foi promulgada pelo então Presidente da República, naquela época Michel Temer, a Lei 13.709/2018, mais conhecida como Lei Geral de Proteção de Dados (LGPD), contendo 65 artigos, sendo originária do Projeto de Lei Complementar (PLC) nº 53/2018. Tal lei foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo. A Lei versa sobre o tratamento de

dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado, englobando um amplo conjunto de operações que podem ocorrer em meios manuais ou digitais.

Ainda, destaca-se que a LGPD, no seu artigo 2º estabeleceu os fundamentos para a devida utilização dos dados pessoais:

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
I - o respeito à privacidade; II - a autodeterminação informativa ;III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Nesse viés, os fundamentos da LGPD estão relacionados ao texto da Constituição Federal de 1988, a saber: Artigos 3, I e II; Artigos 5, 10 e 12; Artigos 7 e 2 Artigo 17; Artigo 219 e Artigo 4, parágrafo 2. Portanto, a LGPD se baseia mais uma vez na proteção e a garantia da privacidade, liberdade, segurança, justiça e desenvolvimento social e econômico das pessoas, garantindo uma melhor segurança jurídica do país. (SOARES 2020. P.17).

Na LGPD, o tratamento de dados pessoais se dão por dois agentes de tratamento, o controlador, que é definido pela Lei como uma pessoa física ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, finalidades e meios de tratamento; e o operador, que é pessoa física ou jurídica, de direito público ou privado, que realizada o tratamento dos dados pessoais em nome do controlador. Outro agente de tratamento dos dados são os chamados “Encarregados”, que são indicados pelo controlador e operador para atuar na comunicação entre o controlador, o titular dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)², assim definido pelo art. 5º, VIII.

Em seu artigo 5º, a LGPD conceitua algumas terminologias que são de grande importância para ter um bom entendimento da referida Lei. Dentre as mais importantes, são elas:

² Será utilizada a forma abreviada da Autoridade Nacional de Proteção de Dados (ANPD) durante todo o texto monográfico.

- a. Dados pessoais: qualquer informação que possa identificar uma pessoa física, como nome, endereço, e-mail, telefone, entre outros.
- b. Tratamento: toda ação realizada com os dados pessoais, como coleta, armazenamento, uso, compartilhamento, entre outros.
- c. Consentimento: autorização prévia e expressa do titular dos dados para que seus dados pessoais sejam coletados, utilizados e compartilhados.
- d. Controlador: a pessoa física ou jurídica responsável pelas decisões referentes ao tratamento dos dados pessoais.
- e. Operador: a pessoa física ou jurídica que realiza o tratamento dos dados pessoais em nome do controlador.
- f. Anonimização: processo de tornar um dado pessoal irreversivelmente impossível de ser associado a um indivíduo.
- g. Eliminação: processo de exclusão de dados pessoais quando não há mais necessidade de mantê-los.
- h. Dado pessoal sensível: dados pessoais que revelam a origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, dados referentes à saúde, vida sexual, entre outros.

A LGPD tem como objetivo proteger os dados pessoais dos cidadãos e garantir a privacidade e segurança desses dados. Para isso, a LGPD estabelece uma série de princípios que devem ser seguidos por empresas e organizações que lidam com dados pessoais, os quais estão arrolados em seu artigo 6º, conforme segue:

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; 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; 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; 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; 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; 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; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - não discriminação: impossibilidade de

realização do tratamento para fins discriminatórios ilícitos ou abusivos; 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.

A LGPD prevê que o tratamento dos dados pessoais deve ser pautado na boa-fé e possuir limites, finalidades, transparência, possibilidade de consulta por titulares, entre outros.

O consentimento deve ser voluntário, informado, específico e inequívoco. Isso significa que a pessoa deve ter a liberdade de escolher se deseja ou não permitir que suas informações pessoais sejam coletadas e deve entender completamente o que está sendo solicitado antes de dar o consentimento. Além disso, o consentimento deve ser específico para cada finalidade de coleta de dados e não deve ser considerado como um requisito para o uso do serviço.

Para Teixeira e Guerreiro (2022, p. 22), o consentimento do titular deverá ser livre e “granularizado”, ou seja, colhido de grão em grão, em que o titular vai consentindo à medida que seus dados são coletados. [...] Para cada finalidade será colhido um consentimento específico, sendo que o titular consente a utilização de seus dados pessoais para um propósito informado previamente, atendendo-se ao princípio da transparência.

O tratamento de dados pessoais sensíveis é uma questão importante na proteção de dados pessoais. Esses dados são considerados sensíveis porque revelam informações sobre a vida privada das pessoas, incluindo informações sobre sua saúde, orientação sexual, religião, etnia, entre outras.

A LGPD define dados pessoais sensíveis como informações que dizem respeito à origem racial ou étnica, convicções religiosas, opiniões políticas, saúde ou vida sexual de uma pessoa, ou informações genéticas ou biométricas. O tratamento desses dados é considerado especialmente delicado, pois eles podem ser usados para discriminação, preconceito ou violação da privacidade dos indivíduos.

O artigo 12 traz em seu texto um ponto de atenção a ser destacado, que dispõe que os dados anonimizados não são considerados dados pessoais. Tal

apontamento da LGPD pode gerar margem a interpretação mais subjetiva e a certo grau de insegurança jurídica. (BRASIL, 2018).

O tratamento de dados pessoais de crianças e adolescentes deve ser realizado com cautela e seguindo algumas regras específicas, como a necessidade de obter o consentimento específico e informado dos pais ou responsáveis legais. Esse consentimento deve ser claro, transparente e informar de maneira adequada a finalidade do tratamento, a forma como os dados serão coletados, armazenados, utilizados e protegidos, além das consequências do não fornecimento dos dados.

A LGPD também proíbe o tratamento de dados pessoais de crianças e adolescentes para fins discriminatórios ou abusivos, bem como a divulgação de informações sobre a rotina e a vida privada desses indivíduos. Além disso, a lei estabelece medidas de segurança para proteção dos dados pessoais de crianças e adolescentes, de forma a garantir a privacidade e a segurança desses indivíduos.

No Brasil, existem diversas leis que garantem a proteção dos direitos da criança e do adolescente, começando com a Constituição Federal que dedica o artigo 227 para este propósito. No entanto, a principal legislação nesse sentido é o Estatuto da Criança e do Adolescente (Lei nº 8.069/90), que estabelece diretrizes específicas para a proteção desses grupos, incluindo a forma como seus dados devem ser tratados, que está condicionada ao consentimento expresso dos pais ou responsáveis.

A proteção de dados pessoais de crianças e adolescentes, conforme previsto no Regulamento Geral sobre a Proteção de Dados (GDPR)³, destaca a importância de garantir a certeza do consentimento dos pais ou responsáveis legais por meio de avanços tecnológicos, a fim de que a autorização seja dada pelo titular das responsabilidades parentais. A simples adoção da classificação etária em termos de uso e privacidade de produtos ou serviços não é suficiente para cumprir o objetivo da norma. Portanto, o controlador deve seguir padrões técnicos ao obter o consentimento para garantir que tenha sido dado pelo responsável legal, ou então o tratamento de dados será considerado ilegal, conforme previsto na lei.

³ Será utilizada a forma abreviada do Regulamento Geral sobre a Proteção de Dados (GDPR) durante todo o texto monográfico.

A LGPD prevê que o término do tratamento de dados ocorre nas seguintes situações:

- a. Quando o objetivo para o qual os dados foram coletados é alcançado;
- b. Quando o titular dos dados solicita a exclusão dos seus dados;
- c. Quando a empresa responsável pelo tratamento de dados deixa de existir;
- d. Quando a obrigação legal ou regulatória que fundamentava o tratamento de dados é cumprida;
- e. Quando o prazo determinado para o tratamento de dados expira.

Após o término do tratamento de dados, a empresa deve adotar medidas técnicas e administrativas para garantir a segurança dos dados pessoais e evitar possíveis vazamentos ou acessos não autorizados. Além disso, a empresa deve comunicar aos titulares dos dados sobre o fim do tratamento e a exclusão dos seus dados pessoais, caso solicitado.

O Capítulo III da LGPD é considerado por muitos especialistas em privacidade e proteção de dados como a principal novidade da lei. É nesse capítulo que são estabelecidos os direitos do titular dos dados pessoais, garantindo que esses titulares tenham maior controle e transparência sobre o tratamento de suas informações.

Para Maldonado e Blum:

O específico conceito de privacidade, em sua origem, referia-se à não interferência estatal quanto à vida dos cidadãos. Posteriormente, com seu amadurecimento, a privacidade passou a ser compreendida em um contexto mais alargado e como um direito mais amplo, tal seja aquele que emerge da prerrogativa de não intromissão sob nenhuma forma e por nenhuma pessoa. [...] Assim, pode-se dizer que a proteção dos dados pessoais é uma das facetas do conceito maior de privacidade, e que brotou e floresceu por decorrência do desenvolvimento tecnológico ocorrido nas últimas décadas.

Um dos principais direitos previstos é o direito de acesso aos dados pessoais. Segundo a LGPD, o titular tem o direito de solicitar à empresa responsável pelo tratamento dos seus dados acesso aos seus dados pessoais, bem como informações sobre o tratamento desses dados. Para o professor Renato Leite Monteiro, esse direito é fundamental para que o titular dos dados possa saber como suas informações estão sendo tratadas pelas empresas e organizações.

Outro direito importante é o direito à retificação. Segundo a LGPD, o titular dos dados pode solicitar a correção de dados pessoais incorretos, incompletos ou desatualizados. Para a professora Patrícia Peck Pinheiro, a retificação é um direito importante para garantir a veracidade e integridade dos dados pessoais. Se um dado estiver incorreto, incompleto ou desatualizado, o titular tem o direito de solicitar a sua correção, evitando assim prejuízos futuros.

Em suma, é fundamental para garantir a proteção dos direitos dos titulares de dados pessoais, concedendo maior transparência e controle sobre o uso de suas informações. Além disso, é importante destacar que o cumprimento dessas disposições é obrigatório para todas as empresas e organizações que tratam dados pessoais, sob pena de sanções previstas na própria LGPD.

O capítulo IV estabelece normas para o tratamento de dados pessoais pelo poder público. O tratamento de dados pessoais deve ser feito com a finalidade de cumprir as atribuições legais ou regulatórias do órgão ou entidade, garantindo a transparência das atividades de tratamento de dados. O poder público deve coletar apenas os dados pessoais estritamente necessários para cumprir a finalidade específica do tratamento e adotar medidas de segurança para proteger os dados pessoais contra acessos não autorizados e vazamentos. Além disso, o compartilhamento de dados pessoais só pode ser feito com outras entidades públicas ou com terceiros mediante autorização legal ou consentimento. O poder público deve permitir o acesso dos titulares dos dados às suas informações pessoais e permitir que esses cidadãos possam corrigir ou excluir suas informações pessoais, quando necessário. (BRASIL, 2018).

De acordo com a referida lei, a transferência internacional de dados só pode ser realizada se o país de destino garantir um nível adequado de proteção de dados pessoais ou se a empresa ou organização que realiza a transferência adotar medidas de segurança para proteger os dados, como cláusulas contratuais específicas ou regras corporativas globais.

Além, exige que a empresa ou organização informe aos titulares dos dados sobre a transferência internacional e as medidas de proteção adotadas. Essa informação deve ser clara, precisa e acessível, permitindo que os titulares dos dados possam decidir se autorizam ou não a transferência.

Caso a empresa ou organização não cumpra as normas previstas na LGPD em relação à transferência internacional de dados, pode ser penalizada com sanções administrativas, como advertência, multa simples ou diária, publicização da infração, bloqueio dos dados pessoais e eliminação dos dados.

Gutierrez (2018) comenta a respeito da transferência internacional de dados:

E chegamos a um elemento crucial para países que estejam elaborando estratégias de desenvolvimento econômico e social. A imposição de restrições legais, regulatórias, ou até mesmo a ausência de infraestrutura física para o fluxo de dados são elementos limitadores para uma estratégia desenvolvimentista na era digital. Por um lado, significam a impossibilidade de acesso às mais atuais tecnologias, prejudicando a competitividade de empresas localizadas no país que exportam produtos e serviços. Por outro, podem dificultar a importação/exportação de serviços – que dependeria de uma migração de profissionais, de servidores e aplicações para o país receptor do serviço. Esse é exatamente o caso de alguns provedores de aplicação que cessaram a oferta de seus produtos no mercado europeu a partir da entrada em vigor do GDPR, em 25 de maio de 2018.

A LGPD define dois agentes de tratamento de dados pessoais: o controlador e o operador. O controlador é a pessoa física ou jurídica responsável pelas decisões referentes ao tratamento de dados pessoais, como a finalidade do tratamento, os dados que serão coletados, a forma como serão utilizados, compartilhados e armazenados. O controlador é quem tem o poder de tomar as decisões mais importantes em relação aos dados pessoais. Já o operador é a pessoa física ou jurídica que realiza o tratamento de dados pessoais em nome do controlador. O operador é responsável por realizar o tratamento de acordo com as instruções do controlador e de maneira segura, preservando a privacidade e a segurança dos dados pessoais.

A LGPD prevê a adoção de medidas técnicas e administrativas para garantir a segurança e a privacidade dos dados pessoais dos titulares. Dentre as medidas técnicas, destacam-se a utilização de criptografia para proteção dos dados, a implementação de sistemas de backup, a utilização de autenticação de acesso e o monitoramento constante dos sistemas. Já as medidas administrativas incluem a realização de treinamentos e capacitações para os funcionários que lidam com dados pessoais, a elaboração de políticas internas de segurança da informação e a nomeação de um encarregado de proteção de dados.

Prevê ainda, a realização de avaliação de impacto à privacidade em casos de tratamentos que possam apresentar riscos elevados aos titulares dos dados. Essa

avaliação consiste em identificar os riscos e avaliar a adequação das medidas de segurança adotadas para minimizar esses riscos. A realização dessa avaliação é obrigatória para o controlador antes de iniciar o tratamento de dados pessoais e pode ser exigida pelas autoridades de proteção de dados em caso de denúncias ou investigações.

A aplicabilidade da lei pode ser consideravelmente melhorada através da adoção de boas práticas e governança, tendo em vista que há diversos setores impactados pela legislação. Uma forma de promover essas boas práticas é por meio da criação de políticas internas de privacidade, instituição de canais de denúncia para proteção de dados, promoção de atividades educativas e treinamentos, bem como a elaboração de manuais e planos para lidar com possíveis vazamentos de dados. Dessa maneira, é possível engajar todos os colaboradores e setores de uma empresa na política de proteção de dados pessoais.

2.2 AS SANÇÕES

As sanções administrativas podem ser aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD) e incluem as seguintes penalidades:

- a. Advertência - é uma medida de caráter educativo, que consiste em alertar o agente de tratamento sobre as infrações cometidas e orientá-lo a corrigi-las.
- b. Multa simples - é uma penalidade pecuniária que pode ser aplicada nos casos de infrações menos graves, cujo valor pode variar de 2% do faturamento da empresa até o limite de R\$ 50 milhões por infração.
- c. Multa diária - é uma penalidade pecuniária aplicada diariamente até que a infração seja corrigida, cujo valor pode variar de 0,1% do faturamento da empresa até o limite de R\$ 50 milhões por infração.
- d. Bloqueio dos dados pessoais - é uma medida que pode ser adotada pela ANPD para interromper o acesso aos dados pessoais em caso de infrações graves.
- e. Eliminação dos dados pessoais - é uma medida que pode ser adotada pela ANPD para eliminar os dados pessoais em caso de infrações graves.

- f. Suspensão parcial ou total do funcionamento do banco de dados ou da atividade de tratamento de dados - é uma medida que pode ser adotada pela ANPD para interromper a atividade de tratamento de dados em caso de infrações graves.

É importante ressaltar que a aplicação das sanções administrativas deve levar em consideração a gravidade e a reiteração das infrações, bem como a capacidade econômica do agente de tratamento de dados. Além disso, a LGPD prevê a possibilidade de recurso administrativo por parte do agente de tratamento de dados.

Observando o princípio constitucional da proporcionalidade, a imputação das sanções deve sempre observar a proporcionalidade como um critério para prevenir e inibir possíveis abusos do poder estatal no momento do exercício de suas funções.

2.3 A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E O CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE (CNPD)

A ANPD é uma entidade da administração pública federal brasileira responsável por zelar pela proteção dos dados pessoais e fiscalizar o cumprimento da LGPD. A ANPD foi criada pela Medida Provisória 869/2018, convertida na Lei 13.853/2019.

O artigo 55 diz que é assegurada autonomia técnica e decisória à ANPD, ou seja, é fundamental para o fortalecimento de sua atuação, que se pretende seja focada na proteção de dados e não em atender desmandos políticos e/ou interesses exclusivamente econômicos. (BRASIL, 2018).

A missão institucional da ANPD é assegurar a mais ampla e correta observância da LGPD no Brasil, e assim, garantir a devida proteção aos direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade dos indivíduos.

Motta (2021) analisa a criação da ANPD, suas atribuições e sua natureza jurídica. Ela ressalta que a ANPD tem por objetivo zelar pela implementação, fiscalização e monitoramento do cumprimento da LGPD. No entanto, ela também menciona que a nova natureza jurídica da ANPD dificulta suas decisões, pois retira

sua tecnicidade diante da dependência da opinião do Poder Executivo e pode ser um dificultador para a aplicação de sanções para o setor público.

O art. 55-J da LGPD estabelece as principais competências da ANPD, dentre algumas, conforme seguem:

- a. Elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;
- b. Fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
- c. Promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;
- d. Estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis;
- e. Promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional.

O CNPD (Conselho Nacional de Proteção de Dados Pessoais e da Privacidade)⁴ é responsável por garantir a proteção dos dados pessoais dos cidadãos brasileiros, além de promover a conscientização sobre a importância da privacidade e da proteção de dados pessoais.

O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD) é composto por 23 membros, sendo 12 representantes do governo, 4 da sociedade civil, 4 do setor empresarial e 3 de entidades acadêmicas. Entre suas atribuições estão: elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; elaborar estudos e recomendações para aperfeiçoar a legislação; e aplicar sanções em caso de infrações à LGPD.

⁴ Será utilizada a forma abreviada do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD) durante todo o texto monográfico.

Suas principais atribuições, conforme o art. 58-B, são:

Art. 58-B. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade: I - propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD; II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; III - sugerir ações a serem realizadas pela ANPD; IV - elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; V - disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população. (BRASIL, 2018).

As Disposições Finais e Transitórias da LGPD estabelecem as regras de transição e adaptação das empresas e órgãos públicos à nova legislação. Entre as principais disposições, podemos destacar que as empresas têm um prazo de 18 meses a partir da entrada em vigor da LGPD (setembro de 2020) para se adequar às novas regras, com a possibilidade de prorrogação por mais seis meses, mediante justificativa fundamentada.

Ainda, a ANPD é criada como órgão responsável por fiscalizar e aplicar sanções em caso de infrações à LGPD; e terá um prazo de dois anos a partir da entrada em vigor da lei para começar a aplicar sanções.

As empresas e órgãos públicos que descumprirem as normas da LGPD estarão sujeitos a sanções que podem incluir advertências, multas de até 2% do faturamento da empresa (limitadas a R\$ 50 milhões por infração), bloqueio ou eliminação dos dados, entre outras.

E ainda, os estados, o Distrito Federal e os municípios têm até 31 de dezembro de 2020 para criar suas próprias autoridades de proteção de dados, que funcionarão em conjunto com a ANPD. Caso isso não aconteça, a ANPD será a responsável por fiscalizar o tratamento de dados pessoais nessas regiões.

A LGPD é um marco significativo no ambiente jurídico e tecnológico, definindo orientações claras para o manejo de dados pessoais no Brasil. Tem como objetivo equilibrar o direito à privacidade dos indivíduos com as necessidades legítimas das empresas e organizações de coletar e usar dados pessoais para propósitos específicos. Ela estabelece princípios como consentimento informado, finalidade específica, transparência, minimização de dados e segurança da informação como componentes fundamentais do tratamento de dados pessoais.

A LGPD também estipula penalidades significativas para o não cumprimento de suas disposições, incentivando a conformidade por parte das empresas e organizações. Além disso, a LGPD institui a ANPD, encarregada de supervisionar e regulamentar a aplicação da lei, fornecendo orientações adicionais.

Está em sintonia com as tendências globais de proteção de dados, como o GDPR da União Europeia, e reflete a importância crescente da privacidade digital em um mundo cada vez mais digitalizado.

No entanto, a implementação efetiva da LGPD requer um esforço conjunto de empresas, organizações, autoridades reguladoras e indivíduos. A conformidade com a LGPD não é apenas uma obrigação legal, mas também uma oportunidade para promover confiança e transparência nas relações entre as partes interessadas.

Na atualidade, os cartórios de registro civil não estão mais apenas registrando nascimentos, casamentos e óbitos. Eles também estão envolvidos na emissão de documentos, como certidões de nascimento e casamento, que contêm informações pessoais sensíveis. Além disso, os avanços tecnológicos têm levado a uma digitalização crescente desses processos, o que torna a proteção dos dados pessoais uma preocupação central.

Nesse contexto, a LGPD impõe obrigações específicas aos cartórios, incluindo a necessidade de obter consentimento informado dos titulares dos dados, a garantia de medidas de segurança adequadas para proteger essas informações e a adoção de práticas de transparência na coleta e uso dos dados. Assim, após o estudo da Lei Geral de Proteção de Dados passa-se a abordar o enquadramento dela nos Cartórios de Registro Civil.

A LGPD busca fortalecer os direitos dos consumidores, proporcionando-lhes maior controle sobre suas informações pessoais e decisões sobre seu uso por empresas, potencialmente aumentando a confiança na sociedade em relação às práticas de manipulação e compartilhamento de dados. No entanto, algumas empresas encaram a legislação como um desafio adicional de conformidade e custos operacionais, pois a necessidade de ajustes internos, implementação de medidas de segurança e garantia de conformidade pode representar um esforço considerável, pois não se enquadrar nela, pode trazer muitos problemas.

3 ENQUADRAMENTO DA LGPD NOS CARTÓRIOS DE REGISTRO CIVIL

Um dos principais ramos do Direito Registral é o registro de pessoas naturais. Nele, incluem-se os registros de nascimento, casamento, óbito e muitos outros registros que tem relação direta com a identidade do indivíduo.

3.1 O QUE É O PESSOA NATURAL E O REGISTRO CIVIL DE PESSOAS NATURAIS

Para Tartuce (2020), a pessoa natural é o ser humano considerado sujeito de direitos e obrigações, dotado de personalidade jurídica e caracterizado pela sua individualidade, existência física e temporal.

Pessoa natural, também conhecida como pessoa física, é um indivíduo considerado sujeito de direitos e obrigações na sociedade. Toda pessoa natural é dotada de personalidade jurídica, ou seja, tem capacidade para exercer direitos e contrair obrigações. Também é caracterizada pela sua individualidade, pois cada ser humano é único e possui características próprias que o diferenciam dos demais. Além disso, a pessoa natural tem uma existência física e temporal, ou seja, nasce em um determinado momento e morre em outro.

Entre os direitos e obrigações das pessoas naturais, pode-se citar o direito à vida, à liberdade, à propriedade, à intimidade e à privacidade, entre outros. As obrigações incluem o cumprimento das leis e normas vigentes, o pagamento de impostos, entre outros deveres civis e sociais.

O registrador civil de pessoas naturais deve realizar o registro e dar publicidade aos fatos e negócios jurídicos que ocorrem na vida de uma pessoa desde seu nascimento até a sua morte. Porém, não se trata do registro de qualquer fato, mas de fatos e negócios jurídicos que interessam à sociedade. (SOUTO; FERREIRA; BARBOZA, 2023).

Foi estabelecido que é fundamental que a população possa registrar seus atos de estado civil em sistemas de registro civil para que se tornem públicos e relevantes do ponto de vista legal. O estado civil é a constatação do estado da pessoa, e o registro civil serve para que os indivíduos possam comprovar sua situação jurídica pessoal, bem como estabelecer seus direitos e deveres. Além disso, os registros civis

permitem que o Estado dê publicidade a esses atos, os quais possuem efeitos que vão além da realidade do indivíduo e impactam a coletividade. Os atos de estado civil são escritos e possuem fé pública, tendo valor probatório diante de todos.

A Lei 6.015/73, a qual rege os registros públicos, no seu artigo 17, dispõe que a publicidade do registro civil de pessoas naturais é formal; isto é, qualquer pessoa pode ter acesso às informações dos registros sem a necessidade de informar o motivo ou interesse no pedido. Essa publicidade é realizada por meio de certidões, nas quais os registradores emitem cópias fiéis e autenticadas das informações constantes formalmente nos livros e registros oficiais. (BRASIL, 1973).

Os registros de pessoas naturais são responsáveis por registrar os principais fatos da vida de uma pessoa, e todos esses registros têm relevância a ponto de se tornarem públicos. Em sua maioria, esses registros possuem natureza declaratória e probatória, ou seja, apenas declaram fatos jurídicos ocorridos. No entanto, alguns registros possuem natureza constitutiva de direitos, o que significa que para que alguns direitos sejam constituídos, devem ser inscritos, como no caso de casamento, divórcio, emancipação, opção de nacionalidade, entre outros.

Além disso, os registros podem sofrer modificações ao longo do tempo, e essas alterações são realizadas por meio das averbações, que são redigidas à margem do assento principal. As averbações têm como finalidade modificar o teor do registro, e qualquer alteração do estado da pessoa deve ser registrada por meio dessas averbações, que indicam a mudança de um estado anterior para outro posterior.

Por exemplo, no caso de divórcio ou separação judicial, essas alterações são inscritas à margem do registro de casamento. É importante ressaltar que uma pessoa que se casa jamais volta a ter o estado civil de solteira, mas sim de separado(a) ou divorciado(a), até que, se for o caso, contraia novo matrimônio. Nesse sentido, a certidão de casamento com as averbações se torna o documento comprobatório do estado civil da pessoa.

As anotações, por sua vez, são registros remissivos a outros atos da vida civil, que são registrados em outros livros. A finalidade dessas remissões é interligar registros, o que garante a informação atualizada sobre o estado da pessoa. Isso

significa que as anotações servem como referências cruzadas para outros registros que são importantes para a compreensão completa do estado civil de uma pessoa.

3.1.1 DO REGISTRO DE NASCIMENTO

O registro de nascimento é o documento inicial e fundamental para a cidadania no Brasil, sendo emitido obrigatoriamente para todo nascituro com vida. Através do registro civil, a condição de pessoa natural é oficializada e suas características pessoais, como nome, filiação, data de nascimento e naturalidade, são comprovadas e tornadas públicas. O registro de nascimento constata e comprova as situações e qualidades pessoais por meio da publicidade, o que garante a oponibilidade erga omnis.

O registro de nascimento deve ser realizado em até 15 (quinze) dias após o nascimento da criança. Em casos de parto em casa ou em localidade distante do cartório, o prazo pode ser estendido para até 45 dias.

Para realizar o registro de nascimento, é necessário comparecer ao cartório de registro civil de pessoas naturais portando os seguintes documentos: declaração de nascido vivo (DNV), documento de identificação dos pais e a certidão de casamento (caso os pais sejam casados). Além disso, os pais devem informar o nome completo da criança e escolher um prenome (nome próprio) para a criança. Observa-se que caso o registrador tiver dúvida quanto ao nome dado à criança (nome com significado pejorativo), o mesmo será encaminhado ao foro competente para a análise do juiz.

Após o registro de nascimento ser realizado, é emitida a certidão de nascimento da criança, que contém informações como nome completo, data de nascimento, nome dos pais, local de nascimento, entre outras informações, e na atualidade, o número de CPF já é gerado no ato do registro, pela serventia extrajudicial. Essa certidão é utilizada para a emissão de outros documentos, como carteira de identidade, passaporte, entre outros.

De acordo com Menelick de Carvalho Netto (2012, p. 29), "O registro de nascimento é um direito fundamental, pois possibilita a aquisição de uma série de outros direitos, como acesso à educação, saúde, previdência social, entre outros. Além disso, é um importante instrumento de cidadania, pois identifica o indivíduo como

parte integrante da sociedade e permite o exercício pleno da sua personalidade jurídica."

3.1.2 DO REGISTRO DE CASAMENTO

De acordo com o art. 1.511 do Código Civil de 2002 (BRASIL, 2002) "Art. 1.511 O casamento estabelece comunhão plena de vida, com base na igualdade de direitos e deveres dos cônjuges."

Na antiguidade, em muitas culturas, o casamento era visto como uma união entre famílias, mais do que entre indivíduos. O objetivo era garantir alianças políticas e econômicas, assegurar a continuidade da linhagem e o patrimônio familiar. As escolhas de casamento eram geralmente feitas pelos pais ou tutores, com pouca ou nenhuma participação dos noivos.

Para Rodrigues (2023), com a chegada do cristianismo, o casamento assumiu uma dimensão religiosa, tornando-se um sacramento, uma união abençoada por Deus. A partir daí, o casamento passou a ser visto também como uma união de amor e devoção mútua, além de seus aspectos práticos e econômicos. Ao longo dos séculos, as práticas matrimoniais mudaram de acordo com a época e a sociedade em que ocorriam. Na Europa medieval, por exemplo, a Igreja passou a controlar o casamento, proibindo a poligamia e exigindo a celebração do matrimônio na presença de um padre. Já na Idade Moderna, o casamento tornou-se mais uma questão de amor e escolha pessoal, com o surgimento do romantismo.

Ainda diz que, com a Revolução Industrial e a urbanização, o casamento deixou de ser visto apenas como uma união entre famílias e passou a ter um papel importante na vida social e econômica. A partir do século XX, as mudanças nas relações de gênero e na sexualidade trouxeram novos desafios e possibilidades para o casamento.

Atualmente, o casamento ainda é uma instituição importante em muitas culturas e sociedades, mas as formas de união e de relacionamento amoroso são cada vez mais diversas e flexíveis. O casamento civil é uma instituição legal, com obrigações e direitos definidos em lei, enquanto outras formas de união, como a união estável e o casamento religioso, têm significados e funções diferentes.

A celebração do casamento possui procedimento específico previsto no Código Civil, a partir do art. 1.533. Após o processo de habilitação dos nubentes e verificada a inexistência de causas impeditivas e suspensivas para o matrimônio, finalmente é chegado o momento da celebração. (BRASIL, 2002).

A celebração do casamento possui procedimento específico previsto no Código Civil, a partir do art. 1.533. De maneira geral, as seguintes etapas costumam ser necessárias para a realização do casamento civil: habilitação: o casal deve comparecer ao cartório e apresentar a documentação necessária para a habilitação do casamento. Isso inclui documentos de identificação, certidão de nascimento ou casamento anterior, comprovante de residência, entre outros; publicação dos proclamas: a intenção de casamento deve ser publicada em um cartório, que antigamente tinha o prazo de pelo menos 15 dias, a fim de permitir que possíveis impedimentos sejam apresentados. Porém, com o E-Proclamas, o casamento pode ser celebrado de um dia para o outro, desde que cumpridas todas as formalidades; celebração do casamento: após o período de publicação dos proclamas e não havendo impedimentos, o casamento pode ser celebrado. Geralmente, a cerimônia é realizada no cartório, na presença do juiz de paz ou de um oficial de registro civil, mas também existe a opção de ser celebrado fora da serventia; registro: após a celebração do casamento, é feito o registro do casamento no cartório, gerando uma certidão de casamento que serve como prova legal da união do casal. (BRASIL, 2002).

Para Souto et al, apud Pereira, 2018, continuam a existir os dois tipos de casamento no ordenamento jurídico brasileiro; porém, para que o casamento religioso tenha efeitos civis, ele deve seguir certos requisitos. Para que gere efeitos civis, o casamento deverá ser celebrado segundo uma seita religiosa reconhecida e deverá atender às exigências formais e substanciais impostas para a validade do casamento civil. Uma vez inscrito, retrotrai nos seus efeitos à data de celebração. Foi mantido o prazo de 90 dias para o registro a partir de sua realização, mediante a comunicação do celebrante ao ofício competente, ou por iniciativa de qualquer interessado desde que tenha sido homologada a habilitação.

A conversão de união estável em casamento é um processo legal que permite que casais que já vivem juntos há algum tempo formalizem a sua união perante a lei.

Essa conversão pode ser feita de forma simples e rápida, sem a necessidade de realizar uma nova habilitação para o casamento.

No Brasil, a conversão de união estável em casamento pode ser feita por meio de um requerimento conjunto do casal, apresentado ao cartório de registro civil. Para isso, é necessário que a união estável já esteja consolidada, ou seja, que o casal conviva de forma pública, contínua e duradoura, com o objetivo de constituir uma família, o qual tenha uma Escritura Pública lavrada pelo Tabelião, e devidamente registrada no Livro “E” no Cartório de Registro Civil.

Ao apresentar o requerimento de conversão, o casal deve apresentar os documentos necessários para a habilitação do casamento, como a identificação, a certidão de nascimento ou casamento anterior e o comprovante de residência.

Após a apresentação do requerimento e dos documentos, o cartório analisa a documentação e, não havendo impedimentos legais, realiza a conversão da união estável em casamento. É importante destacar que não existe celebração do casamento nesse caso, é realizado apenas a emissão da certidão de casamento, após cumpridas as formalidades.

Vale lembrar que a conversão de união estável em casamento pode trazer algumas mudanças na vida do casal, como a alteração do regime de bens, a inclusão do cônjuge como dependente em planos de saúde e seguros, entre outras. Por isso, é importante estar ciente das consequências legais dessa conversão antes de decidir pela formalização da união.

3.1.3 DO REGISTRO DE ÓBITO

A morte é o fim da vida humana e, com ela, extingue-se a personalidade civil (art. 6º do Código Civil).

O Código Civil Brasileiro, em seu artigo 6º, estabelece que a personalidade civil da pessoa natural termina com a morte. Isso significa que, após a morte de uma pessoa física, ela não é mais considerada uma pessoa jurídica e, portanto, não possui mais direitos e obrigações legais. (BRASIL, 2002).

O artigo 77 da referida lei estabelece que todo óbito deverá ser registrado no cartório do registro civil do local em que ocorreu o falecimento, ou no cartório do local de residência da pessoa que faleceu, desde que tenha sido em território nacional.

O registro de óbito é importante porque serve como prova do falecimento da pessoa, e também é utilizado para a obtenção de certidões de óbito, que são documentos necessários para diversos fins, como a abertura de inventários, a habilitação em processos de pensão por morte, entre outros.

Para fazer o registro de óbito, é necessário apresentar ao cartório de registro civil o atestado de óbito, emitido pelo médico ou autoridade competente, e alguns documentos pessoais do falecido, como a certidão de nascimento ou identidade. O prazo para efetuar o registro de óbito é de até 15 dias a partir da data do falecimento.

Conforme art. 2º da Lei no. 8.501, de 30 de novembro de 1992, o cadáver não reclamado junto às autoridades públicas, no prazo de 30 dias, poderá ser destinado às escolas de medicina para fins de ensino e de pesquisa de caráter científico (BRASIL, 1992).

Conforme art. 77, § 2º, da Lei no. 6.015/1973, existe a possibilidade de cremação da pessoa, desde que haja a intenção do próprio indivíduo, porém, deve ser observados algumas formalidades. Caso a pessoa tenha vindo a óbito por causas naturais, o atestado médico deverá ser assinado por dois médicos, porém, se falecida de causa violenta, a cremação somente poderá ser realizada mediante autorização judicial.

De acordo com a doutrina de Nery Júnior, "o registro de óbito é um ato jurídico necessário para a obtenção de uma série de direitos e para o exercício da cidadania, como, por exemplo, o recebimento de pensão por morte e a regularização da situação do patrimônio deixado pelo falecido". (NERY JUNIOR, 2015).

3.2 PROVIMENTOS REGULAMENTANDO O SERVIÇO ELETRÔNICO NOS CARTÓRIOS DE REGISTRO CIVIL

O Provimento 66 do Conselho Nacional de Justiça (CNJ)⁵ é um marco importante na prestação de serviços pelos órgãos de registro civil das pessoas

⁵ Será utilizada a abreviação do Conselho Nacional de Justiça (CNJ) durante todo o texto monográfico.

naturais no Brasil. Este provimento autoriza a celebração de convênios por entidades de classe dos oficiais do registro civil das pessoas naturais, com controle prévio pelas corregedorias dos tribunais de justiça.

O objetivo principal deste provimento é desburocratizar o serviço público prestado ao cidadão brasileiro. Isso significa que o provimento visa tornar os processos mais eficientes e menos complicados para os cidadãos. Além disso, o provimento também visa ampliar o acesso do cidadão brasileiro à documentação civil básica.

Outro aspecto importante do Provimento 66 do CNJ é que ele empreende esforços para que os serviços de registro civil das pessoas naturais implantem a Identidade Civil Nacional e a biometria interligada com o Tribunal Superior Eleitoral e expeçam cadastro de pessoas físicas. Isso significa que o provimento está alinhado com as iniciativas de modernização e digitalização dos serviços públicos no Brasil.

O Sistema Nacional de Informações de Registro Civil (SIRC)⁶ é uma base de dados do Governo Federal que possibilita receber todas as informações de registros civis de pessoas naturais do Brasil. Ele é desenvolvido e hospedado pela Dataprev, operacionalizado pelo INSS e tem sua gestão por meio do Comitê Gestor do SIRC.

No início do século 21, a cultura vigente no país tratava o registro de nascimento como matéria de menor importância a ser resolvido entre família e registrador civil, com a quase total omissão do Estado nessa relação. O sistema privado de registros de nascimento mostrava-se incapaz de alcançar uma grande parte da população. Não havia interligação entre os estabelecimentos de saúde onde nasciam as crianças e os órgãos de registro civil, e tampouco um cadastro nacional único de cartórios.

As ações da União voltadas para a promoção do registro civil de nascimento, enquanto uma política pública, tiveram início efetivo a partir de janeiro de 2003, no âmbito do Programa Fome Zero. A partir daí, o SIRC foi criado para captar, processar, arquivar e disponibilizar dados relativos a registros de nascimento, casamento, óbito e natimorto, produzidos pelos cartórios de registro civil das pessoas naturais. O SIRC

⁶ Será utilizada a abreviação de Sistema Nacional de Informações de Registro Civil (SIRC) durante todo o texto monográfico.

foi instituído pelo Decreto nº 8.270, de 26 de junho de 2014. Além disso, a Recomendação nº 40 do CNJ, publicada em 02 de julho de 2019, dispõe sobre os prazos e informações a serem prestadas ao SIRC pelas serventias extrajudiciais de registro de pessoas naturais.

O Provimento nº 89/2019 do CNJ institui a obrigatoriedade da realização de todos os atos do registro civil de pessoas naturais por meio eletrônico. Com essa medida, os cartórios passaram a utilizar sistemas informatizados para realizar registros de nascimento, casamento e óbito, eliminando o uso de papel e tornando o processo mais ágil e seguro. Além disso, o provimento estabelece a interconexão das bases de dados dos cartórios de todo o país, permitindo que as informações sejam compartilhadas de forma eletrônica entre as serventias.

O Provimento nº 149/2023 do CNJ foi publicado em 30 de agosto de 2023 e instituiu o Código Nacional de Normas da Corregedoria Nacional de Justiça do Conselho Nacional de Justiça – Foro Extrajudicial (CNN/CN/CNJ-Extra), que regulamenta os serviços notariais e de registro. Este provimento foi publicado no Diário da Justiça Eletrônico do Conselho Nacional de Justiça (DJe de 04/09/2023, Edição n. 207/2023, p. 7).

O Código possui 556 artigos e revogou total ou parcialmente, 41 normas publicadas pela CN-CNJ¹. A Exposição de Motivos, assinada pelo Corregedor Nacional de Justiça, Ministro Luis Felipe Salomão, informa que o Código se trata de “uma consolidação de todos os atos normativos do Corregedor Nacional de Justiça, relativamente aos serviços notariais e registrais. O objetivo é eliminar a dispersão normativa atual, que, além de dificultar consultas pelos usuários, é potencialmente nociva à segurança jurídica, seja pela falta de sistematicidade, seja por dificultar a identificação de revogações tácitas, de uma norma por outra”.

A Seção XIII do Provimento 149/2023 do CNJ trata da proteção de dados no âmbito do Registro Civil de Pessoas Naturais (RCPN)⁷. Essa seção estabelece diretrizes para a coleta, armazenamento, tratamento e compartilhamento de dados pessoais no RCPN, em conformidade com a LGPD.

⁷ Será utilizada a abreviação do Registro Civil de Pessoas Naturais (RCPN) durante todo o texto monográfico.

Os principais pontos da seção são:

- a. O RCPN é responsável pelo tratamento de dados pessoais, incluindo dados sensíveis, em razão de suas atribuições legais.
- b. O tratamento de dados pessoais no RCPN deve ser realizado de forma lícita, justa e transparente.
- c. O RCPN deve adotar medidas técnicas e administrativas para proteger os dados pessoais contra acessos não autorizados, destruição, perda, alteração, comunicação ou difusão.
- d. O RCPN deve informar os titulares dos dados pessoais sobre as atividades de tratamento realizadas.
- e. O RCPN deve atender aos pedidos de acesso, correção, eliminação e portabilidade dos dados pessoais;

A seguir, são apresentados os principais artigos da Seção XIII do Provimento 149/2023 do CNJ:

Art. 129. O Registro Civil de Pessoas Naturais é responsável pelo tratamento de dados pessoais, incluindo dados sensíveis, em razão de suas atribuições legais. Art. 130. O tratamento de dados pessoais no Registro Civil de Pessoas Naturais deve ser realizado de forma lícita, justa e transparente. Art. 131. O Registro Civil de Pessoas Naturais deve adotar medidas técnicas e administrativas para proteger os dados pessoais contra acessos não autorizados, destruição, perda, alteração, comunicação ou difusão. Art. 132. O Registro Civil de Pessoas Naturais deve informar os titulares dos dados pessoais sobre as atividades de tratamento realizadas. Art. 133. O Registro Civil de Pessoas Naturais deve atender aos pedidos de acesso, correção, eliminação e portabilidade dos dados pessoais. Art. 134. O CNJ criará uma comissão de proteção de dados no âmbito do Registro Civil de Pessoas Naturais, responsável por propor diretrizes e critérios para a aplicação, interpretação e adequação da Lei Geral de Proteção de Dados às atividades do Registro Civil de Pessoas Naturais.

Com a implementação dos Provimentos Regulamentando o Serviço Eletrônico nos Cartórios de Registro Civil, concluímos um capítulo importante na modernização e digitalização dos serviços cartorários no Brasil. Essas medidas não apenas aumentam a eficiência e a acessibilidade dos serviços de registro civil, mas também representam um passo significativo em direção a um futuro mais digital e conectado.

3.3 PROVIMENTO 134/2022 CNJ, A ADAPTAÇÃO DOS RCPN's À LGPD

Com o objetivo de orientar os cartórios nessa adaptação, o CNJ publicou o Provimento nº 134/2022, que estabelece medidas a serem adotadas pelos cartórios para adequação à LGPD. Essas medidas são importantes para garantir a segurança e a privacidade dos dados pessoais dos cidadãos que utilizam os serviços dos cartórios.

O Provimento 134/2022 é uma importante medida adotada pelo CNJ para garantir a proteção dos dados pessoais dos cidadãos no contexto dos RCPN's. O provimento estabelece diretrizes e medidas a serem adotadas pelos cartórios para garantir o cumprimento das disposições da Lei Geral de Proteção de Dados (LGPD).

Entre as principais medidas previstas no provimento, destacam-se:

- a. Criação de um responsável pela proteção de dados (DPO): os cartórios devem indicar um profissional para atuar como DPO, responsável por garantir a conformidade com as normas de proteção de dados e pela interação com a ANPD;
- b. Realização de avaliação de impacto à proteção de dados (AIPD): os cartórios devem realizar uma AIPD antes de iniciar o tratamento de dados pessoais, a fim de identificar e minimizar possíveis riscos à privacidade dos titulares dos dados;
- c. Adequação dos contratos: os cartórios devem revisar seus contratos com prestadores de serviços e parceiros, para garantir a conformidade com as normas de proteção de dados;
- d. Criação de política de privacidade: os cartórios devem elaborar uma política de privacidade clara e transparente, informando aos titulares dos dados sobre as finalidades e os procedimentos adotados para o tratamento de seus dados;
- e. Adoção de medidas de segurança: os cartórios devem adotar medidas técnicas e organizacionais adequadas para garantir a segurança dos dados pessoais sob sua responsabilidade;
- f. Registro de incidentes: os cartórios devem registrar e notificar os incidentes de segurança que envolvam dados pessoais, e adotar as

medidas necessárias para minimizar os prejuízos aos titulares dos dados.

Para MENDES:

O Provimento 134/2022 do CNJ é um importante instrumento para a adequação dos cartórios de registro civil às disposições da Lei Geral de Proteção de Dados, estabelecendo medidas de governança, segurança, transparência e atendimento aos direitos dos titulares. Trata-se de uma iniciativa que contribui para a proteção dos dados pessoais dos cidadãos e para a garantia de um serviço de qualidade no âmbito dos registros públicos.

O Capítulo I do Provimento 134/2022 do CNJ estabelece as disposições gerais para a adequação dos cartórios à LGPD. Nesse capítulo, são apresentados os objetivos do provimento, que são a proteção de dados pessoais no âmbito dos cartórios, a garantia da segurança jurídica e a uniformização dos procedimentos adotados pelos cartórios. (BRASIL, 2022).

O provimento define o que são dados pessoais e sensíveis, assim como os princípios que devem ser seguidos para o tratamento desses dados, tais como finalidade, adequação, transparência, segurança, entre outros. Além disso, o capítulo também estabelece as obrigações dos cartórios em relação à proteção de dados, como a nomeação de um encarregado pelo tratamento de dados pessoais, a elaboração de um relatório de impacto à proteção de dados pessoais, a adoção de medidas de segurança, entre outras.

O capítulo também define as penalidades aplicáveis em caso de descumprimento das disposições do provimento, que podem variar desde advertência até multa ou até mesmo a suspensão das atividades do cartório. Por fim, o capítulo estabelece a obrigatoriedade da publicação de informações sobre a política de privacidade adotada pelo cartório, de forma clara e acessível ao público.

O Artigo 4º estabelece que os responsáveis pelas delegações dos serviços extrajudiciais de notas e de registro, sejam eles titulares das serventias, interventores ou interinos, são considerados controladores no exercício da atividade típica registral ou notarial. Isso significa que eles têm a responsabilidade de tomar decisões referentes ao tratamento de dados pessoais. O parágrafo único do artigo expande essa definição de controlador para incluir os administradores dos Operadores Nacionais de registros públicos e de Centrais de serviços compartilhados. Eles

também são considerados controladores para fins da legislação de proteção de dados pessoais. (BRASIL, 2022).

O Artigo 5º define o operador, conforme mencionado no artigo 5º da LGPD, como a pessoa natural ou jurídica, de direito público ou privado, que está fora do quadro funcional da serventia e é contratada para prestar serviço que envolve o tratamento de dados pessoais em nome e por ordem do controlador. (BRASIL, 2022).

O Capítulo II do Provimento 134/2022 trata da governança do tratamento de dados pessoais nas serventias, estabelecendo regras para a criação de políticas e procedimentos internos para o tratamento de dados pessoais. (BRASIL, 2022).

O Artigo 6º do referido provimento estabelece medidas a serem adotadas pelas serventias extrajudiciais em âmbito nacional para o processo de adequação à LGPD. Este artigo orienta que, na implementação dos procedimentos de tratamento de dados, o responsável pela serventia extrajudicial deve verificar o porte da sua serventia e classificá-la, de acordo com o Provimento nº 74, de 31 de julho de 2018, da Corregedoria Nacional de Justiça. Além disso, deve observar as regulamentações da ANPD, fazer a adequação à legislação de proteção de dados conforme o volume e a natureza dos dados tratados, e adotar medidas técnicas e organizacionais proporcionalmente à sua capacidade econômica e financeira. (BRASIL, 2022).

O Capítulo IV do Provimento 134/2021 do CNJ estabelece a obrigatoriedade de revisão dos contratos firmados pelas serventias extrajudiciais que envolvam o tratamento de dados pessoais. A revisão deve ser feita para que os contratos estejam em conformidade com as disposições da LGPD e com as exigências estabelecidas no provimento. (BRASIL, 2022).

Nesse sentido, as serventias devem adotar medidas para garantir que os contratos firmados com terceiros para tratamento de dados pessoais incluam cláusulas que estabeleçam a obrigação de cumprimento da LGPD e que prevejam medidas de segurança adequadas para proteção dos dados pessoais.

O Capítulo VI do referido Provimento, trata do Relatório de Impacto à Proteção de Dados Pessoais (RIPD)⁸. Segundo o provimento, os cartórios de registro civil

⁸ Será utilizada a forma abreviada Relatório de Impacto à Proteção de Dados Pessoais (RIPD) durante todo o texto monográfico.

devem elaborar um RIPD, que é um documento que contém uma análise detalhada dos impactos que o tratamento de dados pessoais pode causar aos titulares dos dados, bem como as medidas adotadas para mitigar esses riscos. (BRASIL, 2022).

O RIPD deve ser elaborado em conjunto com o encarregado pelo tratamento de dados pessoais da serventia e deve conter informações como a finalidade do tratamento dos dados pessoais, a descrição dos dados pessoais coletados e armazenados, os riscos envolvidos no tratamento desses dados, as medidas de segurança adotadas para mitigar esses riscos, a base legal para o tratamento dos dados, entre outras informações relevantes.

Além disso, o RIPD deve ser atualizado sempre que houver mudanças relevantes no tratamento de dados pessoais realizado pela serventia ou em caso de ocorrência de incidentes de segurança que possam afetar a proteção dos dados pessoais dos titulares.

O Capítulo VII do Provimento 134/2021 do CNJ trata das medidas de segurança, técnicas e administrativas que devem ser adotadas pelas serventias extrajudiciais para garantir a proteção dos dados pessoais tratados. Essas medidas são fundamentais para assegurar a privacidade, a integridade e a disponibilidade dos dados pessoais, bem como prevenir incidentes de segurança que possam comprometer a sua segurança. (BRASIL, 2022).

Entre as medidas de segurança destacam-se a implementação de sistemas de segurança da informação, que incluem medidas de controle de acesso, criptografia, backup, monitoramento de sistemas, entre outros. Além disso, as serventias devem garantir que todos os funcionários que têm acesso aos dados pessoais recebam treinamentos adequados sobre proteção de dados e boas práticas de segurança da informação.

Já as medidas técnicas incluem a adoção de tecnologias que garantam a segurança dos dados, como a criptografia, a utilização de certificados digitais, a implementação de firewalls, entre outras. É importante ressaltar que a escolha dessas tecnologias deve ser feita de forma criteriosa, levando em consideração as características do ambiente de tratamento de dados pessoais da serventia.

Por fim, as medidas administrativas envolvem a adoção de políticas e procedimentos que garantam a segurança e a privacidade dos dados pessoais. Isso inclui a elaboração de políticas de segurança da informação, a criação de normas internas para o tratamento de dados pessoais, a realização de auditorias periódicas, entre outras medidas.

O Capítulo IX do Provimento 134/2021 do CNJ trata das medidas de transparência e atendimento a direitos de titulares. Ele estabelece que as serventias devem garantir a transparência no tratamento dos dados pessoais, divulgando de forma clara e acessível as informações sobre as finalidades do tratamento, os dados coletados, a forma de armazenamento e os prazos de retenção. (BRASIL, 2022).

Além disso, o capítulo prevê que as serventias devem garantir o atendimento aos direitos dos titulares dos dados pessoais, incluindo o direito de acesso, retificação, exclusão e portabilidade dos dados, bem como o direito de revogação do consentimento.

Para cumprir essas medidas, as serventias devem disponibilizar canais de atendimento ao titular dos dados, tais como telefone, e-mail ou formulário eletrônico, além de fornecer orientações claras e objetivas sobre como exercer os direitos previstos na LGPD. Também devem designar um encarregado de proteção de dados (DPO) e manter registros das solicitações dos titulares de dados, comprovando a efetivação das medidas requeridas.

Essas medidas são essenciais para garantir a transparência e a privacidade dos dados pessoais tratados pelas serventias, assegurando que os titulares possam exercer seus direitos previstos na LGPD.

O Capítulo X do Provimento 134/2022 trata das certidões e compartilhamento de dados com centrais e órgãos públicos. O objetivo é garantir que os dados pessoais contidos nas certidões emitidas pelos cartórios sejam tratados de forma segura e em conformidade com a LGPD. (BRASIL, 2022).

O provimento estabelece que as certidões emitidas pelos cartórios deverão conter informações sobre a finalidade do tratamento dos dados, os direitos dos titulares, o prazo de conservação e as medidas de segurança adotadas para a proteção dos dados.

Além disso, o provimento estabelece que as centrais de serviços eletrônicos compartilhados de registro civil de pessoas naturais deverão garantir a segurança e a privacidade dos dados pessoais dos titulares. Também é previsto que os órgãos públicos terão acesso aos dados pessoais contidos nas certidões apenas quando estritamente necessário e mediante prévia autorização do titular.

O compartilhamento de dados pessoais com órgãos públicos deverá ser realizado por meio de conexão segura e de acordo com as normas estabelecidas pela LGPD e pelo CNJ. O provimento também estabelece que os cartórios deverão manter registros sobre o compartilhamento de dados pessoais e implementar medidas de segurança para evitar acessos indevidos a esses registros.

O capítulo XIII do provimento 134/2022 do CNJ é destinado às disposições relativas ao registro civil de pessoas naturais. Ele estabelece que os cartórios devem adotar medidas para garantir a privacidade e a proteção de dados pessoais dos titulares, em conformidade com a LGPD. (BRASIL, 2022).

O capítulo destaca a importância da segurança na coleta, tratamento e armazenamento dos dados pessoais, bem como na disponibilização das informações aos titulares, observando as normas estabelecidas pela LGPD. Para isso, os cartórios devem adotar medidas de segurança física, lógica e técnica, garantindo que as informações sejam tratadas de forma segura e protegida.

Ainda estabelece, que os cartórios devem fornecer aos titulares das informações o acesso aos seus dados pessoais, assim como a correção de informações incorretas ou incompletas. Além disso, deve ser garantido o direito ao esquecimento, permitindo que os titulares solicitem a exclusão de seus dados pessoais quando não forem mais necessários para a finalidade para a qual foram coletados.

Por fim, o capítulo também estabelece normas para a emissão de certidões, determinando que as informações pessoais contidas nessas certidões devem ser protegidas, evitando o acesso indevido ou o compartilhamento inadequado de dados.

Os provimentos regulamentando o serviço eletrônico nos cartórios de registro civil representam um avanço significativo na modernização e eficiência dos serviços notariais. Eles permitem a digitalização e o acesso eletrônico a documentos e

registros, facilitando a prestação de serviços ao público e aumentando a transparência.

Esses provimentos também estabelecem padrões para a segurança e integridade dos registros eletrônicos, garantindo que os documentos digitais tenham o mesmo valor legal que os documentos físicos. Além disso, eles promovem a cooperação entre diferentes cartórios e órgãos governamentais, permitindo o compartilhamento de informações e a prestação de serviços de forma mais eficiente.

Em suma, a regulamentação do serviço eletrônico nos cartórios de registro civil é um passo importante para a modernização do sistema notarial brasileiro, trazendo benefícios tanto para os profissionais do setor quanto para o público em geral. No entanto, é essencial que se continue a monitorar e avaliar a implementação desses provimentos para garantir que eles estejam atendendo às suas metas pretendidas e para fazer quaisquer ajustes necessários. No próximo capítulo serão estudados e analisados os principais desafios para os Cartórios se adequarem a Lei Geral de Proteção de Dados.

Assim, fica perceptível a importância dos Cartórios de Registro Civil em seus serviços prestados à sociedade, e sem eles teríamos muita dificuldade em ter acesso aos documentos pessoais. Fica nítida a importância do enquadramento da LGPD nos Registros Cíveis, pois assim esses registros estarão protegidos. Pode ser que o acesso a informação fique mais restrito, porém passam a impressão de que os dados estão seguros e protegidos. Algumas pessoas podem apreciar essas regulamentações, vendo-as como uma resposta importante para proteger a privacidade dos cidadãos e garantir que os dados cíveis sejam tratados com transparência e responsabilidade. Isso pode gerar maior confiança na gestão governamental dessas informações sensíveis, promovendo a segurança e o respeito pelos direitos individuais.

Por outro lado, pode haver preocupações sobre os desafios práticos associados à implementação dessas regulamentações nos registros cíveis. Isso inclui a adaptação de sistemas, a garantia de conformidade e a possível sobrecarga para as entidades responsáveis. Algumas pessoas podem temer que a burocracia resultante possa impactar a eficiência do sistema de registros cíveis.

4 OS DESAFIOS PARA OS RCPNs SE ADEQUAREM À LGPD

A Lei é implementada visando salvaguardar os cidadãos durante um período de divulgação intensa de dados e informações individuais. Para atingir esse objetivo, ela coloca a privacidade em destaque, demandando das organizações uma atenção e proteção ampliadas ao lidar com informações pertencentes a terceiros.

Segundo as informações coletadas pela ANOREG – Associação dos Notários e Registradores do Brasil, no ano de 2022, existiam 13.440 Cartórios, distribuídos pelos 5.570 municípios brasileiros. Obrigatoriamente, conforme determina a Lei nº 6.015/1973, cada um deles deve apresentar, no mínimo, uma unidade de Registro Civil para a execução dos atos de nascimento, casamento e óbito.

As informações pessoais protegidas pela lei são necessariamente determinadas ou determináveis. Isto é, quaisquer dados que permitam a identificação de pessoa natural, que os facilitem ou que os tornem possíveis.

Segundo o Tribunal de Justiça de Minas Gerais (2021, p. 16), por dados pessoais entende-se (art. 5º, inc. I):

a) nome civil; b) endereço do domicílio ou residência física; c) endereço eletrônico (e-mail); d) número(s) de documento de identificação e (ou) de cartão de crédito; e) dados de localização de um smartphone ou tablet; f) endereço de Internet Protocol (IP) g) testemunhos de conexão (cookies); h) identificador de publicidade do telefone; i) dados bancários; e (ou) j) informações, fichas, prontuários médicos em meios físicos ou eletrônicos etc.

Também para o Tribunal de Justiça de Minas Gerais (2021, p. 16), o ‘tratamento’ de dados pessoais será permitido nas seguintes hipóteses (art. 7º):

a) a partir do consentimento expresso do usuário; b) quando necessário ao planejamento de política pública; c) nas situações que tenham por objetivo assegurar a vida e a integridade de uma ou mais pessoas naturais, em conjunto; d) na execução de contratos ou nas questões relacionadas ao tema; e) na proteção ao crédito, hipótese em que serão observadas as normas especiais dispostas na legislação consumerista; f) em questões relacionadas à saúde; g) em processos judiciais e administrativos; h) na imposição de obrigação legal para a realização do tratamento; i) em proveito de estudos por órgãos de pesquisa, hipótese em que o acesso será franqueado apenas aos dados, vedada a identificação de seus titulares.

A classe denominada “dados sensíveis” visa conferir proteção especial a dados singulares, tais como raça, etnia, gênero, convicção religiosa, opinião política,

filiação a sindicato, organização de caráter religioso, filosófico ou político, referentes ainda à saúde, à orientação ou à vida sexual, genético ou biomédico, entre outros, de modo a precaver todo e qualquer tipo de ações discriminatórias. Esses dados são submetidos a restrições de publicidade e, naturalmente, não podem ser livremente divulgados (art. 11).

Sob a ótica da LGPD, os dados pessoais sensíveis, que possuem restrições de acesso e devem ser utilizados apenas em circunstâncias predefinidas e para propósitos específicos, carregam consigo informações com potencial para promover ações discriminatórias, seja no âmbito público ou privado. Adicionalmente, a LGPD veda o processamento de dados pessoais sensíveis em nome de interesses legítimos do controlador ou de terceiros, bem como para a proteção de crédito. No entanto, há a ressalva de que é possível tratar dados pessoais sensíveis quando estritamente necessário para cumprir obrigações legais ou regulatórias impostas ao controlador dos dados, para exercer direitos válidos em processos judiciais, administrativos ou arbitrais, ou quando indispensável para a execução de contratos.

O artigo 6 do Provimento 134 do Conselho Nacional de Justiça (CNJ) assume um papel central no contexto da regulamentação e orientação referentes à proteção de dados nos cartórios. Promulgado com o propósito de alinhar os procedimentos cartorários às diretrizes da Lei Geral de Proteção de Dados (LGPD), esse artigo estabelece fundamentos essenciais para o tratamento adequado das informações pessoais em conformidade com as disposições legais, conforme se transcreve a seguir:

Art. 6º Na implementação dos procedimentos de tratamento de dados, o responsável pela serventia extrajudicial deverá verificar o porte da sua serventia e classificá-la, de acordo com o Provimento n. 74, de 31 de julho de 2018, da Corregedoria Nacional de Justiça (Classe I, II ou III), e observadas as regulamentações da Autoridade Nacional de Proteção de Dados ("ANPD"), fazer a adequação à legislação de proteção de dados conforme o volume e a natureza dos dados tratados, e de forma proporcional à sua capacidade econômica e financeira para aporte e custeio de medidas técnicas e organizacionais, adotar ao menos as seguintes providências:

- I – nomear encarregado pela proteção de dados;
- II – mapear as atividades de tratamento e realizar seu registro;
- III – elaborar relatório de impacto sobre suas atividades, na medida em que o risco das atividades o faça necessário;
- IV – adotar medidas de transparência aos usuários sobre o tratamento de dados pessoais;
- V – definir e implementar Política de Segurança da Informação;
- VI – definir e implementar Política Interna de Privacidade e Proteção de Dados;

- VII – criar procedimentos internos eficazes, gratuitos, e de fácil acesso para atendimento aos direitos dos titulares;
- VIII – zelar para que terceiros contratados estejam em conformidade com a LGPD, questionando-os sobre sua adequação e revisando cláusulas de contratação para que incluam previsões sobre proteção de dados pessoais; e
- IX – treinar e capacitar os prepostos.

Em linhas gerais, há três fases em um projeto de adequação à LGPD: a fase de mapeamento, a fase de diagnóstico e a fase de implementação.

4.1 DO MAPEAMENTO DAS ATIVIDADES DE TRATAMENTO

O capítulo III do Provimento 134 do CNJ estabelece princípios fundamentais que devem nortear o tratamento de dados pessoais nos cartórios. Estes princípios abrangem a determinação de finalidades específicas para a coleta e processamento de dados, a transparência nas operações realizadas, a adoção de medidas de segurança, e a assunção de responsabilidade no manuseio desses dados. (BRASIL, 2022).

O mapeamento de dados é definido como a atividade de identificar o banco de dados da serventia, os dados pessoais objeto de tratamento e o seu ciclo de vida, incluindo todas as operações de tratamento a que estão sujeitos, como a coleta, armazenamento, compartilhamento, descarte, e quaisquer outras operações às quais os dados pessoais estejam sujeitos.

Este processo é fundamental para garantir a conformidade com a LGPD. Ele permite que as serventias extrajudiciais compreendam completamente como os dados pessoais são manipulados dentro de suas operações. Isso inclui entender quais dados são coletados, onde e como são armazenados, com quem são compartilhados e como são descartados.

Além disso, o mapeamento de dados ajuda a identificar potenciais riscos à privacidade dos dados e a implementar medidas adequadas para mitigar esses riscos. Isso é particularmente importante dado o volume e a natureza sensível dos dados pessoais que as serventias extrajudiciais geralmente lidam.

Com base no mapeamento, as serventias devem implementar as medidas técnicas e administrativas necessárias para a proteção dos dados pessoais. Essas

medidas devem ser suficientes para proteger os dados de acessos não autorizados, destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Para Santos (2021), o mapeamento de dados, uma etapa crucial para a conformidade com a LGPD, desempenha um papel significativo na identificação de informações essenciais. Isso abrange a categoria dos titulares dos dados pessoais, como clientes, colaboradores e fornecedores. Além disso, o tipo de dados coletados é um ponto sensível, incluindo dados pessoais sensíveis, que possuem proteção aprimorada devido à sua natureza discriminatória, abrangendo origem étnica, crenças religiosas, opiniões políticas e outros. A maneira como os dados pessoais são armazenados também é vital. O mapeamento ajuda a identificar práticas de armazenamento excessivamente longas ou inadequadas, que podem entrar em conflito com os requisitos da LGPD. A legislação requer a eliminação dos dados após o término do tratamento, a menos que a conservação seja necessária por obrigações legais, regulatórias ou outros motivos específicos, observando os critérios definidos na LGPD. Além disso, o mapeamento identifica as lacunas na segurança dos dados, destacando a necessidade de medidas técnicas e administrativas para evitar acessos não autorizados ou situações de perda, alteração e tratamento inadequado.

Ainda, destaca que, o compartilhamento de dados com terceiros também é examinado, sublinhando a importância de informar os titulares sobre o compartilhamento e a necessidade de restrição dessas ações. A fase de mapeamento, frequentemente realizada por meio de análise documental e entrevistas, permite um entendimento holístico do fluxo de dados pessoais. Isso envolve revisar modelos de contratos, políticas de privacidade, manuais de processos internos e regras de acesso a bases de dados. Ao final desse processo, um Relatório de Atividade de Processamento (ROPA)⁹ pode ser elaborado, compilando os resultados do mapeamento e auxiliando na implementação adequada das medidas requeridas pela LGPD.

4.2 DO DIAGNÓSTICO DE AÇÕES PRIORITÁRIAS

⁹ Será utilizada a forma abreviada de Relatório de Atividade de Processamento (ROPA) durante todo o texto monográfico.

Ao conduzir a fase de mapeamento com precisão, juntamente com a elaboração detalhada dos ROPA's, abre-se portas para progredir em direção à etapa de diagnóstico e à definição de ações prioritárias para a adequação à LGPD.

Esta etapa possibilita a identificação de maneira precisa do uso não intencional ou imprevisto de dados pessoais, bem como a identificação dos principais riscos operacionais, permitindo uma análise das áreas mais vulneráveis.

Ao determinar a categoria de dados pessoais envolvidos e a finalidade para a qual são coletados, torna-se possível visualizar potenciais desconformidades com o princípio da necessidade. Esse princípio restringe o tratamento de dados pessoais àquilo que é estritamente necessário para alcançar suas finalidades, garantindo que os dados processados sejam pertinentes, proporcionais e não excessivos em relação aos objetivos do tratamento.

A fase de mapeamento, com a elaboração completa dos ROPA's, desempenha um papel fundamental ao fornecer percepções sobre o panorama de tratamento de dados pessoais dentro da organização. Isso permite uma base sólida para a identificação de áreas que precisam ser aprimoradas para atender aos requisitos da LGPD e garantir a conformidade contínua com os princípios de proteção de dados.

Para Santos (2021), o diagnóstico pode ser visto como uma análise profunda das atividades de processamento de dados da organização, visando entender a extensão do tratamento de dados pessoais em todos os departamentos e processos. Esse exame minucioso dos fluxos de dados revela como os dados são coletados, armazenados, processados e compartilhados. Além disso, destaca se essas práticas estão em conformidade com os princípios estabelecidos na regulamentação de proteção de dados, como a legalidade, finalidade, minimização de dados, exatidão e transparência.

Também comenta que a partir desse diagnóstico, emergem insights claros sobre áreas de não conformidade e possíveis riscos à privacidade dos indivíduos. Pode-se identificar pontos onde a coleta de dados excede a finalidade original, onde as bases legais para processamento são inadequadas ou inexistentes, ou mesmo onde a segurança dos dados está comprometida. A partir dessas análises, a

organização pode determinar as ações prioritárias necessárias para corrigir essas deficiências e melhorar suas práticas de proteção de dados.

O princípio da segurança, destacado na LGPD, estipula que os agentes responsáveis pelo tratamento de dados devem implementar medidas técnicas e administrativas eficazes para garantir a proteção dos dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas, como destruição, perda, alteração, comunicação ou disseminação.

Essas medidas de segurança devem ser consideradas desde a fase de concepção do produto ou serviço até sua implementação. Os sistemas devem ser projetados para atender aos requisitos de segurança, aos padrões de boas práticas e governança, bem como aos princípios gerais definidos não apenas na LGPD, mas também em outras normas regulatórias.

O próximo passo é a elaboração do Relatório de Impacto de Proteção de Dados Pessoais (RIPD), também conhecido como "DPIA" (Avaliação de Impacto à Proteção de Dados). O objetivo desse relatório é realizar uma análise jurídica detalhada dos procedimentos de tratamento de dados pessoais na empresa, identificando possíveis riscos e vulnerabilidades.

O DPIA é um documento que descreve o tratamento de dados pessoais, avalia sua necessidade e proporcionalidade, além de ajudar a gerenciar os riscos associados aos direitos e liberdades individuais. Ele envolve a avaliação dos riscos e a definição de medidas para mitigá-los.

O DPIA é um componente crucial para demonstrar a conformidade com a LGPD, sendo essencial para a construção de um plano de ação. A identificação dos riscos no DPIA é a base para estabelecer ações que visam eliminar ou minimizar esses riscos. A elaboração do plano de ação é uma tarefa interdisciplinar, uma vez que englobará medidas que devem ser implementadas em toda a organização.

Para Junqueira (2022):

O mapeamento preciso das atividades de tratamento de dados pessoais e a elaboração detalhada dos ROPA's são etapas essenciais para a adequação à LGPD. Elas permitem que a organização tenha uma visão clara de suas atividades de tratamento de dados pessoais, o que é fundamental para identificar os principais riscos e desafios relacionados à proteção de dados

personais. Com base nessa compreensão, a organização poderá priorizar as ações necessárias para garantir a conformidade com a LGPD.

A fase de diagnóstico é uma etapa crucial na adequação à LGPD. Esta fase, envolve um entendimento profundo da estrutura da empresa e das práticas adotadas em relação ao tratamento dos dados pessoais. Durante o diagnóstico, o profissional responsável deve investigar Quais são os dados pessoais coletados e a finalidade respectiva, se existe base legal para essa coleta, se a coleta atende aos princípios estabelecidos na LGPD (finalidade, necessidade, transparência, adequação etc.), entre outras.

4.3 DA IMPLEMENTAÇÃO DE MEDIDAS NECESSÁRIAS

O Capítulo VI do Provimento 134 do CNJ trata especificamente do Relatório de Impacto de Proteção de Dados Pessoais (RIPD), também conhecido como DPIA (Avaliação de Impacto à Proteção de Dados). Este capítulo estabelece diretrizes e procedimentos para a elaboração e implementação desse relatório, que desempenha um papel fundamental na garantia da conformidade com a LGPD nos contextos cartorários. (BRASIL, 2022).

Dentro do Capítulo VI, podem ser encontrados os seguintes aspectos:

- a) **Elaboração do RIPD:** O capítulo detalha os passos e os critérios para a elaboração do RIPD. Ele envolve a descrição do tratamento de dados pessoais, a avaliação da necessidade e proporcionalidade do tratamento, bem como a identificação dos riscos e das medidas para mitigá-los.
- b) **Análise de Riscos:** O RIPD é fundamental para a identificação e avaliação dos riscos associados ao tratamento de dados pessoais. Ele ajuda a compreender os impactos potenciais nas liberdades e direitos dos titulares dos dados, bem como a determinar as medidas adequadas para mitigar esses riscos.
- c) **Construção de Plano de Ação:** Com base nas informações fornecidas pelo RIPD, é possível desenvolver um plano de ação que estabeleça as medidas específicas a serem implementadas para lidar com os riscos identificados. Esse plano de ação deve ser interdisciplinar e abordar as áreas relevantes da organização.

- d) Documentação e Comprovação: O capítulo estabelece a importância de documentar todo o processo relacionado ao RIPD, desde sua elaboração até a implementação das medidas de mitigação. Essa documentação serve como evidência de conformidade com a LGPD.
- e) Revisão Periódica: O RIPD não é um documento estático. O capítulo enfatiza a necessidade de revisões periódicas para garantir que as medidas de proteção permaneçam eficazes diante das mudanças nas operações e no ambiente regulatório.
- f) Intervenção do Encarregado de Dados: O capítulo ressalta a importância do Encarregado de Proteção de Dados (DPO) no processo de elaboração e implementação do RIPD, garantindo que todas as etapas estejam em conformidade com as regulamentações de proteção de dados.

A transparência é um dos princípios fundamentais da LGPD, exigindo que os titulares de dados pessoais recebam informações claras, precisas e facilmente acessíveis sobre como seus dados estão sendo tratados e quem são os responsáveis por esse tratamento. Além dos princípios da finalidade, adequação e necessidade, a transparência é um elemento central na estrutura da LGPD.

Diversas medidas podem ser adotadas para assegurar a transparência aos titulares de dados. Uma delas é a criação de um canal eletrônico dedicado ao atendimento de solicitações e reclamações feitas pelos titulares. Também é crucial estabelecer um fluxo bem definido para tratar os direitos dos titulares, desde o momento em que a demanda é recebida até a entrega da resposta correspondente.

Além do canal de atendimento, a minuta do ato normativo do CNJ também sugere outras ações para garantir a transparência. Isso inclui a divulgação de informações em locais de fácil visualização, a disponibilização de informações sobre os procedimentos de tratamento de dados para consulta pública, a inclusão de avisos de privacidade e proteção de dados, e a exibição de avisos de cookies nos sites dos cartórios, fornecendo informações sobre como os dados pessoais estão sendo tratados. Tais medidas visam fortalecer a transparência e proporcionar segurança aos titulares de dados no contexto da LGPD.

Após a elaboração do plano de ação com base nas informações contidas no Relatório de Impacto de Proteção de Dados Pessoais (RIPD), entra-se na fase de implementação, que se adapta às necessidades identificadas nas etapas anteriores e às características específicas de cada empresa.

Conforme Santos (2021), de maneira geral, a fase de implementação abrange:

- a) Revisão e Elaboração de Políticas de Privacidade: Isso envolve tanto políticas internas quanto externas, garantindo que a abordagem de proteção de dados esteja refletida em todos os aspectos da operação.
- b) Elaboração de Cláusulas-padrão: Serão inseridas em contratos com fornecedores ou terceirizados para garantir que as obrigações da LGPD sejam cumpridas.
- c) Revisão de Contratos e Acordos: Serão revistos para lidar com a transferência de dados, podendo envolver a elaboração de cláusulas-padrão ou regras corporativas vinculantes (BCRs).
- d) Plano de Respostas aos Titulares: Define procedimentos para atender às solicitações de informações dos titulares sobre seus dados pessoais.
- e) Plano de Respostas a Incidentes de Vazamento de Dados: Prepara a empresa para lidar com vazamentos de dados, incluindo procedimentos de remediação.
- f) Treinamento dos Colaboradores: Realização de treinamentos para conscientizar os colaboradores sobre a proteção de dados, uma vez que o erro humano pode ser uma fonte significativa de incidentes.

Na fase de implementação, todas as medidas de segurança, tanto técnicas quanto administrativas, são adotadas para proteger os dados pessoais contra acessos não autorizados e situações indesejadas.

É importante ressaltar que a fase de implementação não é uma etapa definitiva. Mesmo após a implementação de todas as ações, é necessário manter um monitoramento constante para assegurar que o tratamento de dados pessoais esteja em conformidade com a LGPD e seus princípios. Esse monitoramento contínuo também permite acionar adequadamente os protocolos de resposta a incidentes de dados pessoais, caso seja necessário.

4.4 MEDIDAS DE SEGURANÇA E TREINAMENTO DE SEUS PREPOSTOS

O Capítulo VII do Provimento 134 do CNJ aborda especificamente as "Medidas de Segurança, Técnicas e Administrativas" a serem adotadas no contexto dos cartórios em conformidade com a LGPD.

Dentro do Capítulo VII, encontram-se os seguintes pontos relevantes (BRASIL, 2022):

- a. **Implementação de Medidas de Segurança:** O capítulo destaca a necessidade de implementar medidas técnicas e administrativas para proteger os dados pessoais contra acessos não autorizados, incidentes acidentais e situações ilícitas, como destruição, alteração, comunicação ou difusão não autorizada.
- b. **Segurança desde a Concepção:** As medidas de segurança devem ser consideradas desde o início do desenvolvimento de produtos ou serviços que envolvam o tratamento de dados pessoais, garantindo que a proteção seja incorporada à sua concepção.
- c. **Princípios de Segurança:** O capítulo alinha as medidas de segurança com os princípios gerais da LGPD, como a finalidade, adequação, necessidade, consentimento, transparência e responsabilidade.
- d. **Avaliação de Riscos:** A avaliação de riscos é enfatizada como uma prática fundamental para determinar as medidas de segurança necessárias. Isso envolve identificar e avaliar riscos potenciais para os direitos e liberdades dos titulares de dados.
- e. **Classificação dos Dados:** A classificação dos dados pessoais conforme sua sensibilidade é abordada, permitindo a adoção de medidas de segurança proporcionais ao nível de risco associado a esses dados.

Ainda pode se destacar os seguintes aspectos:

- a. **Acesso Restrito:** O acesso aos dados pessoais deve ser restrito a indivíduos autorizados, garantindo que apenas aqueles que têm necessidade de acesso possam fazê-lo.
- b. **Política de Segurança:** O capítulo recomenda a elaboração de uma política de segurança que estabeleça diretrizes claras para o tratamento seguro de dados pessoais.

- c. **Monitoramento e Auditoria:** A necessidade de monitorar e auditar regularmente as medidas de segurança é destacada para garantir sua eficácia contínua.
- d. **Responsabilidade:** Os agentes de tratamento de dados devem se responsabilizar pela implementação e manutenção adequadas das medidas de segurança.
- e. **Encarregado de Proteção de Dados (DPO):** O capítulo ressalta a importância do papel do DPO na supervisão das medidas de segurança e na promoção de boas práticas.

Quando se aborda o custo real de um incidente de segurança de dados pessoais, destaque para o relatório da IBM que revela um dado alarmante: em 2021, 23% dos incidentes desse tipo foram causados por erro humano. Esse dado ressalta a urgência da conscientização em relação ao uso responsável e seguro de dados pessoais.

Em outras palavras, se as pessoas que manipulam dados pessoais no cotidiano não compreenderem a importância de proteger esses dados de maneira sólida, o risco de ocorrer falhas humanas aumenta consideravelmente.

Portanto, no contexto da adaptação à LGPD nos cartórios, o treinamento dos profissionais que lidam com dados pessoais não deve ser uma atividade pontual ou superficial. A meta é instaurar uma cultura de proteção de dados, de modo que todos internalizem naturalmente a relevância da proteção de dados em todos os procedimentos realizados no cartório.

Essa abordagem visa a assegurar que a proteção de dados se torne uma parte integrante da mentalidade dos profissionais, de modo que suas ações rotineiras sejam pautadas por boas práticas de segurança de dados. Conscientização contínua e treinamento atualizado são essenciais para reduzir o risco de erros humanos e para criar um ambiente onde a privacidade e a segurança dos dados pessoais sejam prioridades constantes. A criação dessa cultura fortalece a resiliência dos cartórios em relação a ameaças e contribui para uma conformidade duradoura com os princípios da LGPD.

De acordo com Atheniense e Zanata (2023):

O treinamento das pessoas nos RCPN da LGPD é essencial para garantir a conformidade da organização com a lei. Os funcionários devem estar cientes de seus direitos e responsabilidades em relação à privacidade de dados, e devem ser capazes de identificar e mitigar riscos de violação de dados. O treinamento deve ser abrangente e atualizado regularmente para refletir as mudanças na lei e na tecnologia.

O Capítulo VIII do Provimento 134 do CNJ aborda o tema "Treinamento" e estabelece diretrizes detalhadas sobre a necessidade e os aspectos envolvidos na capacitação dos envolvidos no tratamento de dados pessoais em cartórios, em conformidade com a LGPD. (BRASIL, 2022).

O artigo 16 enfatiza a importância dos treinamentos para criar uma cultura de privacidade e proteção de dados pessoais nos cartórios. Ele estabelece que as serventias devem conduzir treinamentos para capacitar todos os envolvidos no tratamento de dados pessoais. Esses treinamentos devem abranger a capacitação de todos os trabalhadores da serventia sobre os procedimentos de tratamento de dados pessoais; a realização de treinamentos com os novos trabalhadores; manutenção de treinamentos regulares para atualização de conhecimentos e procedimentos sempre que necessário; organização de programas de conscientização conduzidos pelo Encarregado e sua equipe, abrangendo todos os trabalhadores e Manutenção de registros que comprovem a participação em cursos, conferências, seminários ou qualquer modo de treinamento fornecido pelo controlador aos operadores e ao Encarregado, incluindo o conteúdo das orientações transmitidas. (BRASIL, 2022)

O parágrafo único do artigo permite que o responsável pela serventia extrajudicial solicite apoio a uma entidade de classe para a capacitação de seus prepostos, reconhecendo a importância da colaboração e orientação externa na promoção da capacitação. (BRASIL, 2022).

O Capítulo VIII do Provimento 134 do CNJ destaca a necessidade crítica de treinamentos contínuos para todos os profissionais envolvidos no tratamento de dados pessoais nos cartórios, visando a garantir uma compreensão sólida dos procedimentos de proteção de dados e a manutenção de uma abordagem consistente de privacidade ao longo do tempo. (BRASIL, 2022).

A Política de Privacidade é um documento elaborado pelo agente de tratamento de dados (seja o controlador ou o operador), contendo uma descrição abrangente das práticas e medidas de privacidade e segurança adotadas no processamento dos dados pessoais, em conformidade com os requisitos da LGPD.

O principal propósito desse documento é promover a transparência, um dos alicerces fundamentais da legislação de proteção de dados. Através da Política de Privacidade, as organizações buscam comunicar claramente aos titulares de dados como seus dados pessoais são tratados, protegidos e utilizados.

A acessibilidade é um requisito crucial para esse documento. Ele deve ser compreensível tecnicamente, utilizando uma linguagem acessível e compreensível para o público em geral. Além disso, deve estar prontamente disponível nos principais canais de comunicação do agente de tratamento, como seu site oficial e redes sociais, garantindo que os titulares de dados possam facilmente encontrá-lo.

4.5 DA TRANSPARÊNCIA

O Capítulo IX do Provimento 134 do CNJ é uma seção fundamental que aborda as "Medidas de Transparência e Atendimento a Direitos de Titulares" no contexto da LGPD aplicada aos cartórios. Esse capítulo desempenha um papel crucial na garantia dos direitos dos titulares de dados pessoais e na promoção de uma cultura de transparência e responsabilidade no tratamento desses dados. (BRASIL, 2022).

Um dos aspectos mais notáveis deste capítulo é a ênfase na importância da transparência. O artigo 17 ressalta que os titulares de dados têm o direito de serem informados sobre como seus dados pessoais estão sendo tratados. Isso inclui detalhes sobre as finalidades do tratamento, os tipos de dados coletados, as bases legais para o tratamento, os direitos dos titulares e informações sobre o Encarregado de Proteção de Dados (DPO), quando aplicável. Esse enfoque na transparência é fundamental para garantir que os titulares estejam cientes de como seus dados estão sendo utilizados e para promover a confiança na forma como os cartórios lidam com suas informações.

Outro ponto relevante é o direito de acesso dos titulares aos seus próprios dados, conforme estabelecido pelo artigo 18. Esse direito permite que os titulares

solicitem e obtenham informações sobre o tratamento de seus dados pessoais, garantindo que eles possam monitorar o uso de suas informações e exercer controle sobre elas.

A importância da precisão dos dados também é abordada no artigo 19, que concede aos titulares o direito de corrigir dados incompletos, inexatos ou desatualizados. Isso é crucial para assegurar que os dados mantidos pelos cartórios sejam precisos e confiáveis.

Além disso, o capítulo trata do direito dos titulares à exclusão de dados (artigo 20), à portabilidade dos dados (artigo 21) e à revogação do consentimento (artigo 22), fornecendo aos titulares um controle significativo sobre suas informações pessoais.

4.6 DA PUBLICIDADE DOS DADOS

O Capítulo X do Provimento 134 do CNJ aborda o tema "Das Certidões e Compartilhamento de Dados com Centrais e Órgãos Públicos" no contexto da LGPD aplicada aos cartórios. Este capítulo estabelece diretrizes específicas para lidar com a emissão de certidões e o compartilhamento de dados pessoais com centrais e órgãos públicos, assegurando a conformidade com as normas de privacidade. (BRASIL, 2022).

O capítulo enfatiza a necessidade de seguir as normas definidas pela ANPD no que diz respeito à emissão de certidões e ao compartilhamento de dados com essas entidades. Isso assegura que essas ações sejam conduzidas dentro dos limites legais e regulamentares, protegendo os dados pessoais dos cidadãos.

Além disso, o capítulo destaca a importância de obter o consentimento específico dos titulares de dados antes de compartilhar informações pessoais com centrais e órgãos públicos, a menos que exista uma base legal que permita o compartilhamento sem consentimento. Isso reforça a importância do consentimento informado e da transparência nas operações de tratamento de dados.

Quando o compartilhamento de dados com centrais e órgãos públicos é necessário para cumprir obrigações legais ou regulatórias, é fundamental que esse compartilhamento seja realizado em conformidade com as leis pertinentes. Isso

garante que os dados sejam compartilhados de acordo com as disposições legais aplicáveis.

A proteção das informações sensíveis presentes nas certidões e documentos emitidos pelos cartórios também é uma preocupação fundamental. O capítulo ressalta a necessidade de implementar medidas de segurança apropriadas para proteger essas informações e prevenir acessos não autorizados, garantindo a confidencialidade dos dados pessoais.

O artigo 35 do Provimento 134/2022 CNJ estabelece que é livre o acesso às informações constantes nos livros de Registro Civil das Pessoas Naturais, por meio de certidões de breve relato, com as informações regulamentadas pelo Provimento n. 63/2017, da Corregedoria Nacional de Justiça, independentemente de requerimento ou de identificação do requerente. (BRASIL, 2023).

Esse artigo é uma importante garantia para o direito à informação. Ele permite que qualquer pessoa possa acessar as informações constantes nos registros de nascimento, casamento e óbito, sem ter que se identificar ou justificar o seu interesse. As informações que podem ser acessadas por meio de certidões de breve relato são: Nome; Data e local de nascimento; Nome dos pais; Data e local de casamento; Nome do cônjuge; Data e local de óbito.

O Artigo 36 do Provimento 134 CNJ estabelece que as certidões de registro civil, incluindo as de inteiro teor, solicitadas pelos próprios interessados, seus representantes legais ou mandatários com poderes especiais, podem ser expedidas sem a necessidade de autorização do Juiz Corregedor Permanente. (BRASIL, 2022).

Isso implica que as pessoas que tenham interesse legítimo em obter certidões de registro civil, como certidões de nascimento, casamento ou óbito, podem fazê-lo diretamente, sem a obrigação de buscar autorização específica do Juiz Corregedor Permanente.

O Artigo 36 do referido provimento estabelece que as certidões de registro civil, inclusive as de inteiro teor, solicitadas pelos próprios interessados, seus representantes legais e mandatários com poderes especiais, podem ser emitidas sem a necessidade de autorização do Juiz Corregedor Permanente. (BRASIL, 2022).

Quando a emissão da certidão for solicitada por terceiros e a certidão contiver dados sensíveis, o parágrafo 1º diz que a expedição somente será realizada com a autorização do juízo competente. Isso significa que, se a certidão contiver informações consideradas sensíveis (como informações sobre saúde, religião, origem racial, entre outras), a expedição da certidão para terceiros exigirá a aprovação do juiz competente.

Após o falecimento do titular dos dados sensíveis, o parágrafo segundo pondera que as certidões mencionadas no Artigo 36 poderão ser fornecidas aos parentes em linha reta, independentemente de autorização judicial. Isso significa que, após o falecimento da pessoa cujos dados sensíveis estão na certidão, os parentes em linha reta (como filhos, pais e avós) podem obter a certidão sem a necessidade de aprovação judicial.

Essas disposições refletem as considerações de proteção de dados e privacidade, permitindo a emissão de certidões de registro civil para os próprios interessados e seus representantes legais de forma ágil, mas estabelecendo salvaguardas especiais para dados sensíveis e considerando a situação após o falecimento do titular dos dados.

O Artigo 39 do Provimento 134 CNJ estabelece as diretrizes para a emissão de certidões em inteiro teor nos registros civis, incluindo os requisitos para requerimento e a forma de assinatura digital. (BRASIL, 2022).

No parágrafo primeiro, a emissão de certidão em inteiro teor exige um requerimento escrito com firma reconhecida do requerente ou com assinatura digital nos padrões ICP-Brasil, no padrão do sistema gov.br ou com assinatura confrontada com o documento de identidade original.

No parágrafo segundo, o reconhecimento de firma não será necessário quando o requerimento for assinado na presença do Oficial ou de um preposto do cartório.

O parágrafo terceiro diz que os requerimentos podem ser enviados por e-mail ou através da Central de Informações do Registro Civil - CRC, desde que assinados digitalmente de acordo com os padrões da ICP-Brasil. A autenticidade e a integridade

da assinatura serão verificadas pelo verificador de conformidade do ITI (Instituto Nacional de Tecnologia da Informação), utilizando o sistema de assinatura gov.br ou assinatura confrontada com o documento de identidade original.

O requerimento para emissão de certidão em inteiro teor deve conter a identificação do requerente, o motivo para solicitar a certidão em inteiro teor, o grau de parentesco com o registrado (caso exista) e se o registrado é falecido ou não, conforme o parágrafo quarto.

Esses requisitos visam garantir a autenticidade, integridade e segurança das certidões em inteiro teor emitidas nos registros civis, ao mesmo tempo em que facilitam a obtenção desses documentos pelos interessados e pela sociedade em geral.

Nesse sentido os artigos 5º e 6º do Provimento 08 CGJ dizem:

Art. 5º - As certidões do Registro Civil das Pessoas Naturais em geral, inclusive as de inteiro teor, requeridas pelos próprios interessados, seus representantes legais ou mandatários com poderes especiais, serão expedidas independentemente de autorização do Juiz de Direito Diretor do Foro ou da Vara dos Registros Públicos, onde houver.

§1º - Considera-se certidão de inteiro teor aquela que reproduz integralmente o conteúdo do registro com suas respectivas averbações e anotações.

§2º - A certidão em relatório, por quesitos, é aquela que contém informações adicionais aos elementos informados na certidão em breve relato, tais como o conteúdo de determinada averbação ou anotação.

§3º - Quando se tratar de certidão requerida por um dos interessados, ainda que presentes dados pessoais de mais uma pessoa, qualquer delas terá legitimidade para o requerimento.

§4º - É possível a expedição de certidão de inteiro teor a terceiros desde que, avaliado o conteúdo, nele não se verifiquem dados sensíveis, sigilosos ou restritos.

§5º - Após o falecimento do titular de dado sensível, as certidões de que trata o caput deste artigo poderão ser fornecidas aos parentes em linha reta e ao cônjuge, independentemente de autorização judicial.

§6º - Não é necessário requerimento ou autorização judicial para emissão de certidão de óbito em nenhuma de suas modalidades, inclusive a terceiros.

Art. 6º - A emissão de certidão em inteiro teor sempre depende de requerimento escrito com firma reconhecida do requerente ou com assinatura digital avançada ou qualificada.

§ 1º - O reconhecimento de firma será dispensado quando o requerimento for firmado na presença do Oficial ou de preposto, ou quando a assinatura puder ser confrontada com o documento de identidade original.

§ 2º - Os requerimentos poderão ser recepcionados por e-mail ou por meio da Central de Informações do Registro Civil-CRC, desde que assinados eletronicamente na forma avançada ou qualificada, com possibilidade de conferência de autenticidade e integridade, ou com assinatura confrontada com o documento de identidade original.

§ 3º - O requerimento de certidão em inteiro teor deverá conter a identificação do requerente, o motivo pelo qual se requer a certidão sob a forma de inteiro teor e o grau de parentesco com o registrado, caso exista, bem como o fato de ser este falecido ou não.

§ 4º A certidão com referência à circunstância de ser legítima a filiação poderá ser fornecida, inclusive a terceiros, independentemente de autorização judicial.

O Provimento CNJ nº 8/2022 revoluciona o acesso a informações nos registros civis, garantindo acesso livre sem requerimentos. Embora benéfico para os titulares de dados, requer responsabilidade ética na busca, bem como segurança e privacidade mantidas pelas serventias extrajudiciais. O formato acessível e a compreensão universal são fundamentais, equilibrando transparência e proteção de dados pessoais.

Como dito, a LGPD é uma legislação complexa e de difícil entendimento, mas vem demonstrando ser crucial para os dias atuais.

A adaptação dos registros civis à LGPD pode ser vista como um desafio significativo, mas necessário para garantir a privacidade e a segurança dos dados dos cidadãos. A implementação dessas regulamentações pode exigir mudanças substanciais nos processos existentes, introdução de medidas de segurança adicionais e treinamento de pessoal.

Em termos práticos, os registros civis precisam estabelecer políticas claras de privacidade, garantir a transparência no tratamento dos dados pessoais e fornecer mecanismos eficientes para que os cidadãos exerçam seus direitos sob a LGPD, como acesso e exclusão de informações. Isso pode envolver investimentos em tecnologia e capacitação de recursos humanos.

Além disso, pode haver desafios na harmonização das normas de proteção de dados com os sistemas já estabelecidos nos registros civis. A integração de práticas compatíveis com a LGPD pode demandar tempo e esforço, especialmente em sistemas mais antigos.

Por outro lado, uma vez superados esses desafios, a conformidade com a LGPD pode fortalecer a confiança dos cidadãos nos registros civis, demonstrando um comprometimento claro com a proteção de seus dados pessoais. Em última análise, a transição para a conformidade com a LGPD nos registros civis pode ser vista como um processo complexo, mas crucial para garantir a segurança e privacidade dos dados dos cidadãos.

5 CONCLUSÃO

À medida que o mundo avança rumo a uma era digital, a proteção dos dados pessoais se torna um pilar fundamental para preservar a privacidade e os direitos individuais dos cidadãos. Neste contexto, a Lei Geral de Proteção de Dados (LGPD) surge como um marco legal crucial no Brasil, reforçando a necessidade de instituições em todos os setores se adaptarem às novas exigências de conformidade e segurança. A principal dificuldade pode residir na compreensão abrangente da LGPD e de suas implicações específicas para o RCPS. Isso inclui o entendimento das definições de dados pessoais, os direitos dos titulares de dados, as responsabilidades das organizações e as penalidades em caso de não conformidade.

Este trabalho se propôs a elucidar caminhos específicos para a aplicação da LGPD nos cartórios de registro civil, um segmento essencial da administração pública que lida com informações pessoais sensíveis e desempenha um papel central na vida dos cidadãos. A análise desse tema complexo revelou que a adequação à LGPD é um desafio considerável para essas instituições, as quais enfrentam uma série de obstáculos em sua jornada rumo à conformidade, dada a natureza específica dos registros de nascimento, casamento e óbito, aliada às tradições e ao legado cultural dos cartórios.

A natureza única dos registros de nascimento, casamento e óbito, aliada às tradições e ao legado cultural dos cartórios, acrescenta uma camada adicional de complexidade à tarefa de garantir conformidade e segurança nos processos de manipulação de dados, somada às tradições e ao legado cultural dos cartórios, torna a adaptação à LGPD uma tarefa que exige sensibilidade e cuidado. No entanto, é uma tarefa que não pode ser adiada, pois a proteção da privacidade dos cidadãos é um direito fundamental e a conformidade legal é imperativa. A LGPD exige uma revisão e adaptação dos processos internos relacionados ao tratamento de dados pessoais. O RCPS deve refletir essas mudanças, garantindo que as práticas estejam em conformidade com a legislação.

Durante a pesquisa, constatou-se que muitos cartórios estão investindo esforços significativos na atualização de seus procedimentos e sistemas para atender às exigências da LGPD. Contudo, ficou evidente que há ainda muito serviço e estudo a serem realizados. A conscientização sobre a importância da proteção de dados e a

implementação de políticas eficazes de privacidade são áreas que demandam atenção contínua por parte de todos os envolvidos.

As medidas de segurança para proteger dados pessoais são um componente crítico. Garantir a implementação de controles de segurança eficazes e documentar essas medidas no RCPS são desafios que as organizações enfrentam. O RCPN deve incluir procedimentos para auditorias regulares e monitoramento contínuo. Isso garante que a organização esteja em conformidade com a LGPD ao longo do tempo, fazendo ajustes conforme necessário.

Além disso, a LGPD nos cartórios de registro civil não se trata apenas de cumprir uma legislação, mas também de aprimorar o relacionamento com os cidadãos e ganhar sua confiança. Os cartórios que conseguirem “abraçar” a LGPD de maneira eficaz não apenas estarão em conformidade com a lei, mas também demonstrarão um compromisso com a privacidade e a segurança dos dados dos brasileiros. Isso permitirá que todos tenham acesso a informações de maneira segura e respeitosa, mantendo um equilíbrio entre os prepostos e os titulares dos dados.

Este estudo destaca a complexidade e a importância da LGPD nos cartórios de registro civil, um tópico que continuará a evoluir à medida que as tecnologias avancem e a conscientização sobre a proteção de dados se intensifique.

Espera-se que os insights e recomendações apresentados aqui contribuam para um debate contínuo e para aprimorar a maneira como essas instituições protegem e gerenciam as informações pessoais dos cidadãos, fortalecendo, assim, a confiança na administração pública e a salvaguarda dos direitos individuais.

Ao longo dos próximos anos mais desafios irão surgir, mas o mais importante é resguardar o direito de todos os cidadãos. Será necessário um esforço em conjunto da sociedade com os poderes públicos, para que todos estejam seguros e protegidos.

REFERÊNCIAS

ATHENIENSE, Alexandre; ZANATA, Rafael. **LGPD: Guia Prático de Compliance**. 2. ed. São Paulo: Fórum, 2023. p. 199.

BRASIL. Conselho Nacional de Justiça. Provimento Nº 66, de 25 de janeiro de 2018. **Dispõe sobre a prestação de serviços pelos ofícios de registro civil das pessoas naturais mediante convênio, credenciamento e matrícula com órgãos e entidades governamentais e privadas**. Diário Oficial da União: seção 1, Brasília, DF, n. 11, 26 jan. 2018. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/2528>. Acesso em: 25 set 2023.

BRASIL. Conselho Nacional de Justiça. Provimento nº 89, de 18 de dezembro de 2019. **Regulamenta o Código Nacional de Matrículas - CNM, o Sistema de Registro Eletrônico de Imóveis - SREI, o Serviço de Atendimento Eletrônico Compartilhado – SAEC, o acesso da Administração Pública Federal às informações do SREI e estabelece diretrizes para o estatuto do Operador Nacional do Sistema de Registro Eletrônico – ONR**. Diário Oficial da União: seção 1, Brasília, DF, 18 dez 2019. Disponível em: <https://atos.cnj.jus.br/files/original173255201912195dfbb44718170.pdf>. Acesso em: 25 set 2023.

BRASIL. Conselho Nacional de Justiça. Provimento nº 134, de 17 de março de 2022. **Dispõe sobre a adequação dos serviços notariais e de registro à Lei Geral de Proteção de Dados Pessoais (LGPD)**. Diário de Justiça Eletrônico, Brasília, DF, 21 mar. 2022. Disponível em: https://atos.cnj.jus.br/files/provimento_134_2022.pdf. Acesso em: 03 maio 2023.

BRASIL. Conselho Nacional de Justiça. Provimento nº 149, de 30 de agosto de 2023. **Institui o Código Nacional de Normas da Corregedoria Nacional de Justiça do Conselho Nacional de Justiça – Foro Extrajudicial (CNN/CN/CNJ-Extra), que regulamenta os serviços notariais e de registro**. Diário da Justiça Eletrônico: seção 1, Brasília, DF, n. 207, 04 set. 2023. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/5243>. Acesso em: 26 set 2023.

BRASIL. Governo Federal. **Guia de Boas Práticas da Lei Geral de Proteção de Dados (LGPD)**. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf. Acesso em: 03 mai. 2023.

BRASIL. **Lei nº 6.015, de 31 de dezembro de 1973**. Dispõe sobre os registros públicos, e dá outras providências. Diário Oficial da União, Brasília, DF, 31 dez. 1973. Disponível em: https://www.planalto.gov.br/ccivil_03/Leis/L6015compilada.htm. Acesso em: 12 jan. 2023.

BRASIL. **Lei nº 8.501, de 30 de Novembro de 1992**. Dispõe sobre a utilização de cadáver não reclamado, para fins de estudos ou pesquisas científicas. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8501.htm. Acesso em: 25 jun. 2023.

BRASIL. **Lei nº 10.406, de 10 de Janeiro de 2002. Institui o Código Civil**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 03 maio 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. Diário Oficial da União, Brasília, DF, 15 ago. 2018.

Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato20152018/2018/lei/L13709.htm. Acesso em: 03 mai. 2023.

BRASIL. Tribunal de Justiça de Minas Gerais. **LGPD e os serviços notariais e de registros - Degustação**. Disponível em:

<<https://www.tjmg.jus.br/data/files/9A/26/E6/AC/30F26710896860676ECB08A8/LGPD%20e%20os%20servicos%20notariais%20e%20de%20registros%20-%20Degustacao.pdf>>. Acesso em: 23 ago. 2023.

CARVALHO NETTO, Menelick de. **Registro civil de nascimento e identificação da paternidade**. 1. ed. São Paulo: Saraiva, 2012. p. 29.

GUTIERREZ, Andrei. **Transferência Internacional de dados & estratégias de desenvolvimento nacional**. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Ópice. *Comentários ao GDPR*. São Paulo: Thomson Reuters Brasil, 2018. p. 218.

IBM. **Estudo IBM: consumidores pagam o preço por violações de dados**. IBM Comunica, 2022. Disponível em: <https://www.ibm.com/blogs/ibm-comunica/estudo-ibm/>. Acesso em: 25 fev. 2023.

Junqueira, G. (2022). **A LGPD: Guia de Adequação para Empresas**. 1ª ed. São Paulo: Editora Saraiva. p. 20.

JUSBRASIL. **Art. 17 - Capítulo III - Dos Direitos do Titular - LGPD - Lei Geral de Proteção de Dados Pessoais Comentada**. Disponível

em: <https://www.jusbrasil.com.br/doutrina/secao/art-17-capitulo-iii-dos-direitos-do-titular-lgpd-lei-geral-de-protecao-de-dados-pessoais-comentada/1198081154>.

Acesso em: 25 set. 2023.

MENDES, Flávio Luiz. **Proteção de dados pessoais nos cartórios de registro civil**. In: *Revista do Instituto de Registro Civil das Pessoas Naturais do Brasil*, ano 4, n. 8, p. 20-29, jan./jun. 2022.

MOTTA, Clara Amédée Péret. **A ANPD e a preocupação com sua natureza jurídica**. Disponível em: <https://www.migalhas.com.br/depeso/344752/a-anpd-e-a-preocupacao-com-sua-natureza-juridica>. Acesso em: 25 set. 2023.

NERY JÚNIOR, Nelson. **Código Civil comentado**. 15. ed. rev., atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2015. p. 375.

PENA, Rodolfo Ferreira Alves. **MUNDO EDUCAÇÃO. Era da Informação**. UOL. Disponível em: <https://mundoeducacao.uol.com.br/geografia/era-informacao.htm>.

Acesso em: 25 set. 2022.

PINHEIRO, Patrícia Peck. **PROTEÇÃO DE DADOS PESSOAIS: COMENTÁRIOS À LEI N. 13.709/2018 (LGPD)**. São Paulo: Editora Saraiva, 2021. E-book. ISBN 9786555595123. Disponível em:

<https://integrada.minhabiblioteca.com.br/#/books/9786555595123/>.

Acesso em: 03 maio 2023.

RODRIGUES, Lucas de Oliveira. **História do casamento.** Disponível em: <https://mundoeducacao.uol.com.br/sociologia/historia-casamento.htm>. Acesso em: 25 fev. 2023.

SANTOS, Fernanda Cristina Soares. **Adequação à LGPD na prática.** Lage Portilho Jardim. Disponível em: <https://lageportilhojardim.com.br/blog/adequacao-a-lgpd/>. Acesso em: 26 set 2023

SANTOS, Fernanda Cristina Soares. **LGPD: entenda a nova Lei Geral de Proteção de Dados.** Lage Portilho Jardim. Disponível em: <https://lageportilhojardim.com.br/blog/lgpd/>. Acesso em: 26 set 2023.

SOARES, Rafael Ramos. **Lei de Proteção de Dados – LGPD: Direito à Privacidade no Mundo Globalizado, 2020 (Graduação em Direito)** – Pontifícia Universidade Católica de Goiás.

SOUTO, Fernanda R.; FERREIRA, Gabriel B.; BARBOZA, Maytê R. T M.; et al. **Registro civil de pessoas naturais e o registro empresarial.** São Paulo: Grupo A, 2021. E-book. ISBN 9786556901060. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786556901060/>. Acesso em: 03 maio 2023.

TARTUCE, Flávio. **Manual de Direito Civil - Volume Único.** 7ª ed. São Paulo: GEN Atlas, 2020.

TEIXEIRA, Ana Carolina Grzybowski; GUERREIRO, João Pedro Pedrosa. **Adequação à LGPD e aos princípios da proteção de dados pessoais no Brasil.** Revista de Direito Digital e Compliance, v. 6, n. 2, p. 57-71, 2021.

TEIXEIRA, Tarcísio; GUERREIRO, Ruth M. **Lei Geral de Proteção de Dados Pessoais (LGPD): Comentada Artigo por Artigo.** São Paulo: Editora Saraiva, 2022. E-book. ISBN 9786555599015. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555599015/>. Acesso em: 03 maio 2023.

TEIXEIRA, Tarcísio; STINGHEN, João R.; LIMA, Adrienne Correia de; et al. **LGPD e Cartórios: Implementação e Questões Práticas.** São Paulo: Editora Saraiva, 2021. E-book. ISBN 9786555597967. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555597967/>. Acesso em: 03 maio 2023.