ReGeo ISSN: 2177-3246

A CITAÇÃO E A INTIMAÇÃO ELETRÔNICA NA LGPD: UM ESTUDO SOBRE A VALIDADE E A SEGURANÇA JURÍDICA DA CITAÇÃO E INTIMAÇÃO ELETRÔNICA SOB A ÓTICA DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

ELECTRONIC SERVICE OF PROCESS AND NOTIFICATION UNDER THE LGPD: A STUDY ON THE VALIDITY AND LEGAL SECURITY OF ELECTRONIC SERVICE OF PROCESS AND NOTIFICATION FROM THE PERSPECTIVE OF THE GENERAL DATA PROTECTION LAW (LGPD)

NOTIFICACIÓN Y EMPLAZAMIENTO ELECTRÓNICO CONFORME A LA LGPD: UN ESTUDIO SOBRE LA VALIDEZ Y LA SEGURIDAD JURÍDICA DE LA NOTIFICACIÓN Y EL EMPLAZAMIENTO ELECTRÓNICO DESDE LA PERSPECTIVA DE LA LEY GENERAL DE PROTECCIÓN DE DATOS (LGPD)

https://doi.org/10.56238/revgeov17n7-012

Data de submissão: 18/05/2026 **Data de publicação:** 02/07/2026

Beatriz Jacinto Xavier
Bacharel em Direito
Instituição: Faculdade UNISAPIENS
E-mail: drabeatrizxavier@gmail.com

Pedro Henrique Moreira Simões
Doutorando em Direito
Instituição: Faculdade FADISP
E-mail: pedrohmsimoes@yahoo.com.br

RESUMO

Este artigo analisa o dilema entre a celeridade processual e a proteção de dados na era digital, focando na validade e segurança jurídica da citação e intimação eletrônica. A pesquisa, de natureza qualitativa, exploratória e descritiva, utilizou uma metodologia robusta que incluiu a análise de doutrina, legislação, jurisprudência e normativos do CNJ. A investigação demonstrou que, apesar dos avanços do Processo Judicial Eletrônico e do seu marco legal (Lei nº 11.419/2006 e CPC/2015), os sistemas de comunicação do Poder Judiciário ainda enfrentam desafios significativos para se adequarem plenamente à Lei Geral de Proteção de Dados (LGPD). Falhas na conformidade com os princípios de segurança, finalidade e transparência podem comprometer a validade jurídica dos atos e expor dados pessoais a riscos. O estudo conclui que a segurança e a validade das comunicações eletrônicas não se resumem à mera automação, mas dependem de um arcabouço técnico-jurídico robusto capaz de garantir a autenticidade e a irretratabilidade dos atos. Nesse sentido, são propostas medidas como a padronização de protocolos de segurança, a maior transparência na coleta de dados e a capacitação dos operadores do Direito, assegurando que a modernização da justiça não comprometa os direitos fundamentais dos cidadãos. A digitalização do Poder Judiciário trouxe um dilema: como equilibrar a celeridade e efetividade do processo eletrônico com os requisitos de privacidade e proteção de dados da LGPD? Este artigo científico analisa a validade e a segurança jurídica de atos processuais essenciais, como a citação e a intimação eletrônica, confrontando-os com as exigências da Lei Geral de Proteção de Dados Pessoais (LGPD). A pesquisa, baseada em uma metodologia bibliográfica e jurisprudencial, investigou a conformidade dos sistemas judiciais brasileiros e concluiu que, embora haja um avanço tecnológico considerável, ainda persistem falhas que podem comprometer a segurança das informações e, consequentemente, a validade jurídica das comunicações. A falta de protocolos de segurança

padronizados, a coleta de dados desnecessários e a ausência de transparência são os principais desafios. O estudo reitera a necessidade de um arcabouço técnico e jurídico robusto para garantir a proteção de dados. Por fim, propõe medidas para aprimorar a segurança e a validade das comunicações eletrônicas, destacando a urgência de capacitação dos operadores do Direito e a implementação de protocolos de segurança mais rigorosos nos sistemas judiciais.

Palavras-chave: Celeridade Processual. Proteção de Dados (LGPD). Citação e Intimação Eletrônica. Segurança Jurídica e Processo Judicial Eletrônico (PJe).

ABSTRACT
This article analyzes the dilemma between procedural celerity and data protection in the digital era, focusing on the validity and legal certainty of electronic service of process and summons. This qualitative, exploratory, and descriptive research employed a robust methodology, including the analysis of legal doctrine, legislation, case law, and National Council of Justice (CNJ) regulations. The investigation demonstrated that, despite the advancements of the Electronic Judicial Process and its legal framework (Law No. 11,419/2006 and the 2015 Civil Procedure Code), the Judiciary's communication systems still face significant challenges in fully complying with the General Data Protection Law (LGPD). Non-compliance with the principles of security, purpose, and transparency may compromise the legal validity of acts and expose personal data to risks. The study concludes that the security and validity of electronic communications go beyond mere automation, depending on a robust technical-legal framework capable of guaranteeing the authenticity and irretraceability of procedural acts. Consequently, measures are proposed such as the standardization of security protocols, greater transparency in data collection, and specialized training for legal practitioners, ensuring that the modernization of justice does not compromise citizens' fundamental rights.

Keywords: Procedural Celerity. Data Protection (LGPD). Electronic Service of Process. Legal Certainty. Electronic Judicial Process.

RESUMEN
Este artículo analiza el dilema entre la rapidez procesal y la protección de datos en la era digital, centrándose en la validez y la seguridad jurídica de las citaciones y notificaciones electrónicas. La investigación, de carácter cualitativo, exploratorio y descriptivo, empleó una metodología sólida que incluyó el análisis de la doctrina, la legislación, la jurisprudencia y la normativa del Consejo Nacional de Justicia (CNJ). La investigación demostró que, a pesar de los avances en el Proceso Judicial Electrónico y su marco jurídico (Ley n.º 11.419/2006 y CPC/2015), los sistemas de comunicación del Poder Judicial aún enfrentan importantes desafíos para adaptarse plenamente al Reglamento General de Protección de Datos (RGPD). El incumplimiento de los principios de seguridad, finalidad y transparencia puede comprometer la validez jurídica de los actos y exponer los datos personales a riesgos. El estudio concluye que la seguridad y la validez de las comunicaciones electrónicas no se limitan a la mera automatización, sino que dependen de un marco técnico-jurídico sólido capaz de garantizar la autenticidad y la no repudiación de los actos. En este sentido, se proponen medidas como la estandarización de protocolos de seguridad, una mayor transparencia en la recopilación de datos y la capacitación de profesionales del derecho, garantizando que la modernización de la justicia no comprometa los derechos fundamentales de los ciudadanos. La digitalización del Poder Judicial ha planteado un dilema: ¿cómo equilibrar la rapidez y la eficacia del proceso electrónico con los requisitos de privacidad y protección de datos de la LGPD (Ley General de Protección de Datos de Brasil)? Este artículo científico analiza la validez y la seguridad jurídica de actos procesales esenciales, como las citaciones y notificaciones electrónicas, comparándolos con los requisitos de la LGPD. La investigación, basada en una metodología bibliográfica y jurisprudencial, investigó la conformidad de los sistemas judiciales brasileños y concluyó que, si bien existe un avance tecnológico considerable, persisten deficiencias que pueden comprometer la seguridad de la información y, por consiguiente, la

validez jurídica de las comunicaciones. La falta de protocolos de seguridad estandarizados, la recopilación de datos innecesarios y la ausencia de transparencia son los principales desafíos. El estudio reitera la necesidad de un marco técnico y jurídico sólido para garantizar la protección de datos. Finalmente, propone medidas para mejorar la seguridad y validez de las comunicaciones electrónicas, destacando la urgente necesidad de capacitar a los profesionales del derecho e implementar protocolos de seguridad más rigurosos en los sistemas judiciales.

Palabras clave: Eficiencia Procesal. Protección de Datos (LGPD). Citación y Notificación Electrónicas. Seguridad Jurídica y Proceso Judicial Electrónico (PJE).

1 INTRODUÇÃO

1.1 A DIGITALIZAÇÃO COMO FERRAMENTA DE CELERIDADE PROCESSUAL

A celeridade processual, um dos pilares do Poder Judiciário contemporâneo, encontrou na digitalização uma ferramenta essencial para sua efetivação. A Lei do Processo Judicial Eletrônico (Lei n. 11.419/2006) marcou a transição do papel para o ambiente virtual, estabelecendo as bases para um sistema jurídico mais ágil e acessível (BRASIL, 2006) [1] . Nesse cenário, a citação e a intimação, atos processuais fundamentais que garantem o exercício do contraditório e da ampla defesa, foram gradualmente incorporadas ao meio eletrônico, otimizando o fluxo de informações e reduzindo o tempo de tramitação dos litígios.

No entanto, a eficiência tecnológica não pode se sobrepor à segurança jurídica. Conforme ensina Marinoni (2015) [2] , o processo eletrônico, embora célere, não pode violar os princípios constitucionais do devido processo legal, sob pena de nulidade dos atos. A citação e a intimação eletrônicas, ao manipularem dados pessoais sensíveis — como nome, endereço e, em alguns casos, informações sobre saúde ou patrimônio do indivíduo —, entraram em uma zona de atenção crítica com a entrada em vigor da Lei Geral de Proteção de Dados Pessoais (LGPD).

A LGPD (Lei n. 13.709/2018) [3] estabelece um conjunto de regras e princípios para o tratamento de dados pessoais, com o objetivo de proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade (BRASIL, 2018). Embora a lei preveja bases legais para o tratamento de dados no contexto de um processo judicial (art. 7º, inciso VI), ela também impõe a observância de princípios como a finalidade, a necessidade e, sobretudo, a segurança (art. 6º, incisos I, II e VII).

A relevância deste estudo, portanto, reside na problemática central que se estabelece: como conciliar a celeridade e a efetividade das comunicações processuais eletrônicas com os rigorosos requisitos de proteção de dados impostos pela LGPD? A questão é de suma importância para a academia e para a prática jurídica, pois a validade e a segurança de atos processuais essenciais dependem da conformidade dos sistemas judiciais com a nova legislação. A modernização, nesse contexto, deve garantir que os direitos e garantias dos cidadãos não sejam comprometidos.

[1] BRASIL. Lei nº 11.419, de 19 de dezembro de 2006. Dispõe sobre a informatização do processo judicial. Diário Oficial da União, Brasília, DF, 20 dez. 2006.
[2] MARINONI, Luiz Guilherme. O Processo Eletrônico: Eficiência sem garantias?. Revista de Processo, v. 240, p. 1-15, 2015
[3] 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.

1.2 A VALIDADE DAS COMUNICAÇÕES PROCESSUAIS ELETRÔNICAS À LUZ DA LGPD

O questionamento sobre a validade e a segurança jurídica das comunicações processuais eletrônicas, como a citação e a intimação, à luz da Lei Geral de Proteção de Dados Pessoais (LGPD), é central para o Direito Processual contemporâneo. A questão vai além da simples digitalização de atos e se aprofunda na conformidade deles com os princípios e garantias constitucionais, que agora são reforçados pelo novo marco legal da proteção de dados.

Em teoria, a validade da citação e da intimação eletrônica é assegurada pela Lei nº 11.419/2006 [4] , que trata da informatização do processo judicial. No entanto, essa validade depende intrinsecamente da segurança jurídica do ato. Conforme adverte Fredie Didier Jr. (2018) [5] , "a adoção do processo eletrônico não significa a dispensa das garantias processuais, mas a sua adaptação ao novo ambiente". Isso implica que a citação eletrônica só é válida se for capaz de assegurar, de forma incontestável, a ciência inequívoca do réu sobre o processo, garantindo o contraditório. A fragilidade de um sistema, a possibilidade de fraude ou a falta de um registro seguro de entrega podem, portanto, tornar o ato nulo.

A LGPD (Lei nº 13.709/2018) [6] adiciona uma camada de complexidade a esse cenário. Embora o Poder Judiciário tenha a prerrogativa de tratar dados pessoais para a realização de políticas públicas ou para a execução de uma competência legal (art. 7º, incisos III e VI), ele não está isento de seguir os princípios da lei. A LGPD, conforme aponta Doneda (2019) [7] , impõe ao operador de dados, neste caso o próprio Judiciário, a responsabilidade de adotar "medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações de destruição, perda, alteração, comunicação ou difusão indevida". Portanto, a segurança jurídica de uma citação eletrônica não se restringe à sua comprovação técnica, mas também à proteção dos dados pessoais nela contidos.

1.3 A CONFORMIDADE DOS SISTEMAS JUDICIAIS COM A LGPD

A questão da conformidade dos sistemas de comunicação do Poder Judiciário é mais delicada e não tem uma resposta única, pois varia entre os tribunais. De modo geral, pode-se afirmar que os sistemas do Judiciário ainda enfrentam desafios significativos para se adequarem plenamente à LGPD.

O principal problema reside na falta de um protocolo unificado de segurança. A maioria dos tribunais utiliza o Diário de Justiça Eletrônico (DJe) ou sistemas próprios de intimação, os quais, em grande parte, foram desenvolvidos antes da vigência da LGPD. Isso levanta dúvidas sobre: finalidade e

[4] BRASIL. Lei nº 11.419, de 19 de dezembro de 2006. Dispõe sobre a informatização do processo judicial. Diário Oficial da União, Brasília, DF, 20 dez. 2006.
[5] DIDIER JR., Fredie. Curso de direito processual civil: teoria do processo judicial, processo de conhecimento e procedimento comum. v. 1. Salvador: JusPodivm, 2018.
[6] 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.
[7] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. São Paulo: Editora Revista dos Tribunais, 2019.

necessidade dos sistemas que coletam apenas os dados estritamente necessários para a comunicação processual;

A segurança e integridade das informações são garantidas por meio de uma criptografia forte aplicada a todas as intimações. O acesso é estritamente restrito a usuários autorizados, garantindo que apenas aqueles que realmente precisam da informação possam acessá-la. A robustez do sistema é assegurada por um mecanismo de login e senha avançado.

Em termos de transparência, o sistema judicial garante que o titular dos dados, o cidadão, tenha pleno conhecimento de como suas informações são tratadas, processadas e armazenadas, em total conformidade com o princípio da transparência estabelecido pela legislação.

A jurisprudência ainda é incipiente, mas já se observa o debate em torno de nulidades processuais decorrentes de falhas nas comunicações eletrônicas. Embora não haja uma declaração categórica de que os sistemas judiciais violam a LGPD [8] , o risco existe, e ele se materializa quando uma falha no sistema compromete o direito fundamental de defesa, como uma intimação que não é entregue, ou um dado sigiloso que é exposto.

Em suma, a validade das comunicações eletrônicas está condicionada à sua segurança jurídica, que, por sua vez, deve ser garantida pelas proteções oferecidas pela LGPD. Os sistemas judiciais, portanto, precisam ser revisados e aprimorados para garantir que a inovação tecnológica não venha a custo da segurança e dos direitos dos cidadãos.

2 ANÁLISE VALIDADE E A SEGURANÇA JURÍDICA DAS CITAÇÕES E INTIMAÇÕES ELETRÔNICAS EM FACE DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

O presente estudo tem como objetivo geral analisar a validade e a segurança jurídica das citações e intimações eletrônicas em face da Lei Geral de Proteção de Dados Pessoais (LGPD). Para tal, desdobram-se os seguintes objetivos específicos:

a) compreender os conceitos de citação e intimação eletrônica no contexto do processo judicial;
b) examinar os principais requisitos da LGPD aplicáveis às comunicações processuais, como a finalidade, a necessidade, a segurança e a transparência;
c) avaliar se os sistemas e procedimentos do Poder Judiciário brasileiro estão em conformidade com as exigências da LGPD; e
d) propor medidas ou diretrizes para aprimorar a segurança e a validade jurídica das comunicações eletrônicas no âmbito judicial.

[8] 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.

A citação e a intimação são atos processuais que garantem ao cidadão o direito fundamental ao devido processo legal, ao contraditório e à ampla defesa. A citação é o ato que dá ciência ao réu sobre a existência de um processo, convocando-o a integrar a relação jurídica processual (BRASIL, 2015) [9] . Já a intimação busca dar conhecimento a qualquer pessoa envolvida no processo sobre atos e termos processuais (DIDIER JR., 2018) [10] .

Com o advento do processo judicial eletrônico, a comunicação se digitalizou, permitindo que esses atos sejam realizados de forma automatizada e remota. A Lei nº 11.419/2006 estabeleceu a validade jurídica das comunicações eletrônicas (BRASIL, 2006) [11] , desde que observadas as formalidades legais. A validade, contudo, não se restringe à simples informatização, exigindo que o sistema utilizado garanta a autenticidade, a integridade e a irrefutabilidade da entrega da comunicação.

O tratamento de dados pessoais no âmbito judicial, embora respaldado pelo art. 7º, inciso VI, da LGPD [12] , deve obedecer aos princípios do art. 6º. A colisão de normas entre a celeridade processual e a proteção de dados é inevitável. Nesse sentido, os sistemas de citação e intimação eletrônica devem observar, rigorosamente, os seguintes requisitos: O tratamento de dados deve se limitar ao propósito de dar ciência dos atos processuais. Qualquer coleta de dados que exceda essa finalidade – por exemplo, a requisição de informações não essenciais à identificação da parte – constitui desvio de finalidade (DONEDA, 2019) [13] . A LGPD exige a adoção de medidas técnicas e administrativas aptas a proteger os dados de acessos não autorizados e de incidentes de segurança (BRASIL, 2018) [14] . Isso implica que os sistemas de comunicação eletrônica devem ser robustos, utilizando criptografia e outras tecnologias para garantir que as informações da citação não sejam interceptadas ou adulteradas. O titular de dados deve ter acesso a informações claras sobre como seus dados são tratados (BINENBOJM, 2020) [15] . Isso significa que os tribunais devem informar, de maneira acessível, como os dados são coletados, armazenados e utilizados para a citação ou intimação.

A avaliação da conformidade dos sistemas de comunicação processual do Poder Judiciário com a LGPD revela uma realidade complexa e, por vezes, deficiente. Embora muitos tribunais tenham

[9] BRASIL. Lei nº 13.105, de 16 de março de 2015. Código de Processo Civil. Diário Oficial da União, Brasília, DF, 17 mar. 2015

[10] DIDIER JR., Fredie. Curso de direito processual civil: teoria do processo judicial, processo de conhecimento e procedimento comum. v. 1. Salvador: JusPodivm, 2018.

[11] BRASIL. Lei nº 11.419, de 19 de dezembro de 2006. Dispõe sobre a informatização do processo judicial. Diário Oficial da União, Brasília, DF, 20 dez. 2006

[12] 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.

[13] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. São Paulo: Editora Revista dos Tribunais, 2019.

[14] 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

[15] BINENBOJM, Gustavo. O princípio da transparência na Lei Geral de Proteção de Dados. In: SARLET, Ingo Wolfgang; MENEZES, Joyceane Bezerra de; LIMA, Cíntia de Freitas (coords.). LGPD e a Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2020.

investido em plataformas de intimação eletrônica, a segurança nem sempre é garantida. O uso de senhas fracas, a falta de autenticação de múltiplos fatores e a ausência de auditorias regulares expõem o sistema a vulnerabilidades.

A falta de um padrão nacional de segurança, aliada à ausência de uma autoridade específica para fiscalizar o tratamento de dados no judiciário, cria um ambiente de incerteza. A jurisprudência, por sua vez, tem se manifestado de forma pontual, mas ainda não há uma consolidação que resolva de forma definitiva as questões de validade em caso de falha de segurança. Nesse contexto, a validade do ato pode ser questionada e, em caso de vício, culminar na anulação do processo.

Para solucionar as falhas existentes, é imperativo que o Poder Judiciário adote medidas proativas. Propõe-se: Padronização dos Protocolos de Segurança: O Conselho Nacional de Justiça (CNJ) deve criar e implementar um protocolo de segurança de dados para todos os tribunais, exigindo o uso de criptografia de ponta a ponta e a autenticação de múltiplos fatores para o acesso aos sistemas de intimação; Aprimoramento da Capacitação: É essencial capacitar magistrados, servidores e advogados sobre a importância da proteção de dados e as melhores práticas de segurança da informação. Auditorias Periódicas: Os sistemas devem ser submetidos a auditorias de segurança regulares por órgãos independentes, a fim de identificar e corrigir vulnerabilidades. Garantia de Transparência e Acesso: O Judiciário deve criar portais de transparência que expliquem, de forma clara, a política de tratamento de dados pessoais, permitindo que o cidadão exerça seus direitos.

A análise da validade e da segurança jurídica das comunicações processuais eletrônicas revela que, apesar dos avanços tecnológicos, a conformidade plena com a LGPD ainda é um desafio. A segurança do processo eletrônico e, por conseguinte, a sua validade, dependem da rigorosa observância dos princípios de finalidade, necessidade e, acima de tudo, segurança. A implementação de medidas concretas e a adoção de uma cultura de proteção de dados são cruciais para que o processo judicial eletrônico continue a ser um instrumento de celeridade, sem jamais comprometer a segurança e os direitos fundamentais do cidadão.

3 METODOLOGIA

A presente pesquisa adota uma abordagem metodológica predominantemente qualitativa, por se debruçar sobre a análise e interpretação de normas jurídicas, conceitos e princípios, sem a necessidade de quantificação de dados. O método qualitativo, conforme defendido por Minayo (2014) [16] , é ideal para o estudo de fenômenos sociais complexos, permitindo uma compreensão aprofundada das dinâmicas entre o Direito e a tecnologia no contexto do processo judicial.

[16] MINAYO, Maria Cecília de Souza. O desafio do conhecimento: pesquisa qualitativa em saúde. 14. ed. São Paulo: Hucitec, 2014.

A pesquisa é, ao mesmo tempo, exploratória e descritiva. O caráter exploratório se justifica pela necessidade de aprofundar a compreensão sobre a problemática da colisão entre o Processo Judicial Eletrônico e os princípios da LGPD, um tema ainda em consolidação no cenário jurídico brasileiro. Como apontado por Gil (2002) [17] , a pesquisa exploratória visa a familiarizar-se com o tema, tornando-o mais claro e permitindo a construção de hipóteses. Em contrapartida, o viés descritivo visa a descrever as características do fenômeno em estudo, analisando os sistemas e procedimentos de citação e intimação eletrônica atualmente utilizados pelo Poder Judiciário, sem a intenção de estabelecer relações de causalidade direta.

Para a coleta de dados, a pesquisa se baseará em um rigoroso levantamento de fontes secundárias, o que a caracteriza como uma pesquisa bibliográfica e documental. As fontes de pesquisa incluem: doutrina especializada: Serão consultados livros e artigos de juristas renomados nas áreas de Direito Processual Civil e Direito Digital, com foco em autores que abordam o processo eletrônico, a citação e intimação, bem como a proteção de dados pessoais, como Fredie Didier Jr., Luiz Guilherme Marinoni e Danilo Doneda; Legislação: O estudo será fundamentado na análise da Lei Geral de Proteção de Dados Pessoais (LGPD) (Lei nº 13.709/2018), na Lei do Processo Judicial Eletrônico (Lei nº 11.419/2006) e no Código de Processo Civil (Lei nº 13.105/2015); Jurisprudência: Serão examinadas decisões de tribunais superiores e estaduais que discutem a validade da citação e intimação eletrônica, bem como a aplicação da LGPD no âmbito judicial, a fim de identificar o entendimento do Judiciário sobre o tema;Normativos do Conselho Nacional de Justiça (CNJ): Será analisado o arcabouço normativo do CNJ, como as Resoluções e Recomendações que regulamentam o Processo Judicial Eletrônico e a gestão de dados nos tribunais.

A análise dos dados será realizada por meio da técnica de análise de conteúdo, permitindo a identificação de padrões e categorias nas fontes consultadas para, assim, construir os argumentos e as conclusões do trabalho.

4 REFERENCIAL TEÓRICO

4.1 O PROCESSO JUDICIAL ELETRÔNICO E A CITAÇÃO/INTIMAÇÃO

A evolução do direito processual no Brasil tem sido marcada pela busca por celeridade, eficiência e acessibilidade à justiça. Nesse contexto, a informatização do Poder Judiciário surgiu como uma resposta aos desafios impostos pela morosidade e pela burocracia do sistema tradicional, em papel. Como aponta Marinoni (2015) [18] , o processo eletrônico representa uma mudança de paradigma, visando a otimizar a prestação jurisdicional e a diminuir os custos para o cidadão e para o Estado. A

[17] GIL, Antônio Carlos. Como elaborar projetos de pesquisa. 4. ed. São Paulo: Atlas, 2002.
[18] MARINONI, Luiz Guilherme. O Processo Eletrônico: Eficiência sem garantias?. Revista de Processo, v. 240, p. 1-15, 2015.

transição não é apenas tecnológica, mas também cultural, exigindo a adaptação de todos os operadores do direito.

A informatização do processo judicial brasileiro foi formalizada com a sanção da Lei n. 11.419/2006, que dispôs sobre o uso de meios eletrônicos na tramitação de processos judiciais, na comunicação de atos processuais e na formação e acompanhamento de autos (BRASIL, 2006) [19] . Essa legislação foi o ponto de partida para a criação do Processo Judicial Eletrônico (PJe), plataforma unificada que permite o trâmite de ações de forma 100% digital.

Posteriormente, o Código de Processo Civil de 2015 (CPC) reforçou a validade e a obrigatoriedade do processo eletrônico, estabelecendo-o como regra geral (BRASIL, 2015) [20] . O CPC dedicou um capítulo inteiro à prática de atos processuais eletrônicos, validando a citação e a intimação por meio eletrônico, em especial para empresas públicas e privadas que mantêm cadastro nos sistemas dos tribunais.

Nesse cenário, como destaca Didier Jr. (2018) [21] , a tecnologia não substitui os princípios processuais, mas os instrumentaliza, permitindo que a citação eletrônica, por exemplo, seja tão ou mais eficaz que a sua versão em papel.

A citação e a intimação, atos essenciais para o exercício da ampla defesa e do contraditório, ganharam novos contornos no ambiente digital. A citação eletrônica, para ser considerada válida, deve garantir a ciência inequívoca do réu sobre a demanda, assegurando que a comunicação foi entregue e recebida com sucesso. Da mesma forma, a intimação eletrônica, que dá ciência sobre os atos e termos do processo, depende de um sistema confiável que comprove a data e a hora da leitura.

Os principais desafios residem na necessidade de um arcabouço técnico e jurídico que assegure a autenticidade, a integridade e a irrefutabilidade da comunicação. O ato eletrônico, diferentemente do físico, não possui a materialidade da assinatura ou do carimbo de recebimento. Por isso, a validade jurídica desses atos está atrelada à robustez do sistema que os gerencia. A garantia de que a mensagem não foi adulterada e de que o destinatário é, de fato, a pessoa que deveria ser citada ou intimada é crucial para evitar a nulidade do processo, conforme a lição de Marinoni (2015) [22] .

[19] BRASIL. Lei nº 11.419, de 19 de dezembro de 2006. Dispõe sobre a informatização do processo judicial. Diário Oficial da União, Brasília, DF, 20 dez. 2006.
[20] BRASIL. Lei nº 13.105, de 16 de março de 2015. Código de Processo Civil. Diário Oficial da União, Brasília, DF, 17 mar. 2015
[21] DIDIER JR., Fredie. Curso de direito processual civil: teoria do processo judicial, processo de conhecimento e procedimento comum. v. 1. Salvador: JusPodivm,
[22] MARINONI, Luiz Guilherme. O Processo Eletrônico: Eficiência sem garantias?. Revista de Processo, v. 240, p. 1-15, 2015.

Apesar dos avanços, a implementação ainda apresenta obstáculos. A falta de padronização entre os sistemas dos diferentes tribunais, as falhas de segurança e a necessidade de capacitação dos operadores do direito e dos jurisdicionados são desafios a serem superados.

4.2 A LGPD E O TRATAMENTO DE DADOS PESSOAIS NO PODER JUDICIÁRIO

A entrada em vigor da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, marcou um divisor de águas no direito brasileiro, ao estabelecer um arcabouço normativo para o tratamento de dados pessoais (BRASIL, 2018) [23] . O principal objetivo da lei, como aponta Doneda (2019) [24] , é proteger a privacidade e os direitos fundamentais de liberdade e de desenvolvimento da personalidade de cada indivíduo. A LGPD, portanto, não é apenas um conjunto de regras técnicas, mas um reflexo de princípios que visam a garantir maior controle do cidadão sobre suas próprias informações.

A LGPD é fundamentada em dez princípios que devem ser observados em qualquer operação de tratamento de dados. Dentre eles, destacam-se a finalidade (o tratamento deve ter propósitos legítimos e específicos), a necessidade (a coleta deve se limitar ao mínimo indispensável para a finalidade) e a segurança (devem ser adotadas medidas técnicas e administrativas para proteger os dados). Esses princípios são, na prática, o guia para a conformidade de qualquer órgão ou empresa.

Para que o tratamento de dados seja lícito, ele deve ser amparado por uma das dez bases legais previstas no art. 7º da LGPD. As mais comuns incluem o consentimento do titular, o cumprimento de uma obrigação legal ou regulatória e a execução de um contrato. A lei também garante aos titulares de dados uma série de direitos, como o de acesso, correção, anonimização e portabilidade de seus dados, bem como o direito de revogar o consentimento a qualquer momento [25] .

Embora a LGPD seja aplicável a todas as esferas, a sua aplicação no contexto do Poder Judiciário apresenta desafios e nuances específicas. A atividade judicial, por sua própria natureza, envolve a coleta e o tratamento de uma vasta quantidade de dados pessoais, muitos deles sensíveis. A proteção desses dados deve ser equilibrada com o interesse público na transparência e na efetividade da justiça. Como ressalta Binenbojm (2020) [26] , a atividade judicial, por ser essencial ao Estado

[23] 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.
[24] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. São Paulo: Editora Revista dos Tribunais, 2019.
[25] 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.
[26] BINENBOJM, Gustavo. O princípio da transparência na Lei Geral de Proteção de Dados. In: SARLET, Ingo Wolfgang; MENEZES, Joyceane Bezerra de; LIMA, Cíntia de Freitas (coords.). LGPD e a Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2020.

Democrático de Direito, demanda um tratamento de dados que, por vezes, se sobrepõe a alguns direitos do titular, mas sem jamais violar a dignidade humana.

A grande questão, portanto, reside em como o Poder Judiciário pode cumprir seu papel de persecução judicial e pacificação social sem ferir os princípios da LGPD. Os desafios são claros: garantir a segurança dos dados armazenados em sistemas eletrônicos, evitar a exposição indevida de informações sigilosas e assegurar que o tratamento dos dados seja sempre pautado pela finalidade processual.

A LGPD, de forma acertada, prevê bases legais específicas para o tratamento de dados pessoais por órgãos públicos, inclusive o Poder Judiciário. Os principais dispositivos que legitimam essa atividade são:

> Art. 7º, inciso VI: Estabelece que o tratamento pode ser realizado para "a execução de políticas públicas, por órgãos públicos, nos termos da lei ou de regulamentos". No caso do judiciário, a atividade de prestar a tutela jurisdicional se enquadra perfeitamente nesse inciso.
>
> Art. 7º, inciso IX: Permite o tratamento quando "necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais". A atividade judicial, ao buscar a justiça e a segurança jurídica, se encaixa nesse critério.
>
> Art. 4º, inciso III: Esse artigo é crucial, pois retira a aplicação da LGPD "para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, ou de atividades de investigação e repressão de infrações penais". Embora isso não signifique total isenção, a doutrina entende que essas atividades possuem um regime jurídico próprio, o que reforça a autonomia da atuação judicial em casos específicos.

A LGPD, portanto, não proíbe o tratamento de dados pelo Poder Judiciário, mas exige que ele seja feito com responsabilidade, transparência e segurança. A validade da comunicação processual eletrônica, nesse contexto, dependerá cada vez mais da capacidade dos sistemas judiciais de conciliar a eficiência tecnológica com a proteção dos direitos fundamentais garantidos pela lei.

5 ANÁLISE CRÍTICA

5.1 A COLISÃO ENTRE A CELERIDADE PROCESSUAL E A PROTEÇÃO DE DADOS

A modernização do Poder Judiciário trouxe um dilema: como conciliar a busca por celeridade processual com a garantia da proteção de dados? A eficiência, meta prioritária do processo eletrônico, pode, paradoxalmente, comprometer a segurança e a privacidade, pilares da Lei Geral de Proteção de Dados Pessoais (LGPD). Esse conflito revela uma tensão entre dois princípios igualmente importantes, exigindo uma análise cautelosa para que a inovação não venha à custa de direitos fundamentais.

O processo eletrônico, ao substituir o papel por arquivos digitais, otimiza o trâmite dos litígios. Contudo, essa digitalização acarreta um novo conjunto de riscos. O volume de dados pessoais tratados — informações sobre partes, testemunhas, endereços, e até dados sensíveis como históricos médicos — aumenta exponencialmente. Conforme aponta Doneda (2019) [27] , a coleta e o armazenamento de grandes bancos de dados criam um ambiente propício a vazamentos e usos indevidos, caso não haja medidas de segurança robustas.

A citação e a intimação eletrônica são exemplos claros desse conflito. A busca por agilidade na comunicação pode levar à adoção de sistemas que não garantem a devida proteção. Uma intimação enviada por e-mail ou aplicativo de mensagem, por exemplo, pode ser interceptada, exposta a terceiros ou acessada por quem não é o real destinatário, comprometendo a privacidade das informações e, potencialmente, a segurança jurídica do ato.

A problemática da colisão entre celeridade e proteção de dados já se reflete na jurisprudência brasileira, especialmente em casos que envolvem a validade de atos processuais. Embora a doutrina e a legislação de proteção de dados sejam recentes, o debate sobre a validade da comunicação eletrônica já é antigo e agora ganha uma nova dimensão.

Um exemplo notável é a jurisprudência que discute a validade da citação por WhatsApp. O tema já chegou ao Superior Tribunal de Justiça (STJ), que em algumas decisões têm validado a citação, desde que acompanhada de prova inequívoca de que o réu recebeu a mensagem, leu-a e teve ciência do conteúdo (STJ, 2017) [28] . No entanto, o Tribunal de Justiça do Rio Grande do Sul (TJRS, 2020) [29] já se manifestou de forma contrária em casos de intimação para audiência por meio do aplicativo, declarando-as nulas por entender que a ferramenta não oferece a segurança necessária para comprovar a efetiva ciência do ato. Essas divergências demonstram a ausência de um consenso e a fragilidade de sistemas que não foram criados com o objetivo de proteger dados, reforçando a necessidade de um sistema oficial e seguro.

A LGPD adiciona uma camada de complexidade a essa discussão. Qualquer falha que leve a um vazamento de dados durante uma comunicação processual pode, em tese, levar a uma penalidade administrativa imposta pela Autoridade Nacional de Proteção de Dados (ANPD), além de sanções cíveis e penais. A busca por eficiência não pode se sobrepor aos princípios da LGPD, em especial o da

[27] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. São Paulo: Editora Revista dos Tribunais, 2019.
[28] SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). REsp 1646271/MG. Relator: Ministro Luis Felipe Salomão, Quarta Turma, julgado em 06/06/2017, DJe 08/08/2017.
[29] TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL (TJRS). Agravo de Instrumento nº 70083547901. 22ª Câmara Cível, julgado em 29/01/2020

segurança (art. 6º, inciso VII), exigindo que o Poder Judiciário, como controlador de dados, adote todas as medidas técnicas e administrativas necessárias para proteger as informações (BRASIL, 2018) [30] .

5.2 AVALIAÇÃO DOS SISTEMAS ATUAIS DE CITAÇÃO E INTIMAÇÃO

A digitalização do Poder Judiciário brasileiro, impulsionada pela Lei nº 11.419/2006 [31] , resultou na criação de sistemas como o Diário de Justiça Eletrônico (DJe) e diversas plataformas de intimação eletrônica. No entanto, a mera substituição do papel pela tela não garante a conformidade desses sistemas com os rigores da Lei Geral de Proteção de Dados Pessoais (LGPD). A avaliação de sua adequação aos princípios da LGPD, como a segurança, a finalidade, a necessidade e a transparência, revela tanto avanços quanto lacunas que precisam ser abordadas.

O princípio da segurança, previsto no artigo 6º, inciso VII da LGPD, exige que o controlador de dados adote medidas técnicas e administrativas para proteger os dados pessoais de acessos não autorizados e de situações de destruição, perda ou difusão indevida (BRASIL, 2018) [32] . Nesse aspecto, os sistemas do Poder Judiciário têm evoluído, mas ainda apresentam desafios.

A maioria das plataformas de intimação eletrônica utiliza criptografia para proteger a comunicação entre o servidor e o usuário, e a autenticação é realizada por meio de login e senha ou, em casos mais seguros, por certificação digital. Contudo, a efetividade dessas medidas varia. A falta de protocolos unificados e a ausência de auditorias de segurança regulares podem expor o sistema a vulnerabilidades. A jurisprudência, embora incipiente, já demonstrou preocupação com a segurança de plataformas, como no caso da intimação via aplicativos de mensagens, em que o Superior Tribunal de Justiça (STJ) condicionou a validade do ato à comprovação inequívoca do recebimento pelo destinatário, em face da insegurança da ferramenta (STJ, 2017).

Os princípios de finalidade e necessidade, dispostos no artigo 6º, incisos I e III da LGPD, impõem que o tratamento de dados pessoais seja realizado para propósitos legítimos, específicos e informados ao titular, com a coleta restrita ao mínimo indispensável para a sua realização.

Os sistemas de intimação e citação eletrônica, por sua natureza, tratam dados pessoais com a finalidade específica de comunicar atos processuais. No entanto, a conformidade desses sistemas pode ser questionada em relação à necessidade. Muitas plataformas de cadastro de partes solicitam dados que não são estritamente necessários para a comunicação processual, como informações de contato

[30] 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.
[31] BRASIL. Lei nº 11.419, de 19 de dezembro de 2006. Dispõe sobre a informatização do processo judicial. Diário Oficial da União, Brasília, DF, 20 dez. 2006.
[32] 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.

secundárias ou detalhes da vida privada do indivíduo. Como alerta Doneda (2019) [33] , a coleta de dados excessivos pode caracterizar um desvio de finalidade, violando a LGPD.

O princípio da transparência, previsto no artigo 6º, inciso VI da LGPD, garante aos titulares o direito de obter informações claras, precisas e acessíveis sobre o tratamento de seus dados. No âmbito judicial, a aplicação desse princípio é crucial, mas nem sempre é efetiva.

O cidadão, parte de um processo, muitas vezes não tem acesso facilitado a informações sobre como o tribunal armazena, protege e utiliza seus dados pessoais para fins de comunicação. As políticas de privacidade dos sites dos tribunais, quando existem, nem sempre são claras e compreensíveis para o público leigo. Segundo Binenbojm (2020) [34] , a transparência é fundamental para construir a confiança entre o Estado e o cidadão. No caso do Poder Judiciário, a ausência de transparência pode gerar insegurança jurídica, fazendo com que o jurisdicionado não saiba se seus dados estão sendo protegidos ou se a comunicação processual é realmente segura.

A análise demonstra que, embora os sistemas de comunicação eletrônica do Poder Judiciário representem um avanço na celeridade processual, sua plena conformidade com a LGPD ainda exige aprimoramentos. A segurança, a finalidade e a transparência precisam ser reforçadas para que a digitalização não comprometa a proteção de dados e, por conseguinte, a validade e a segurança jurídica de atos processuais essenciais.

5.3 O DESAFIO DA AUTENTICIDADE E DA IRRETRATABILIDADE

A transição do processo judicial em papel para o meio eletrônico trouxe inúmeros ganhos em celeridade e eficiência. Contudo, essa evolução gerou um dilema central no que se refere aos atos de comunicação: como garantir, em um ambiente virtual, a autenticidade e a irretratabilidade da citação e da intimação. Em outras palavras, a grande questão é assegurar que a comunicação foi, de fato, entregue e recebida pelo destinatário correto, e que o ato não pode ser negado posteriormente.

A autenticidade de um documento ou comunicação eletrônica é a garantia de sua origem. No processo tradicional, essa garantia é dada por elementos como o carimbo do oficial de justiça ou a assinatura do recebedor. No meio digital, essa tarefa é realizada por meio de ferramentas como a certificação digital. A Lei nº 11.419/2006, que instituiu o Processo Judicial Eletrônico, já reconhecia a validade do uso de assinaturas eletrônicas e digitais, que possuem a mesma força probatória dos documentos em papel (BRASIL, 2006) [35] .

[33] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. São Paulo: Editora Revista dos Tribunais, 2019.
[34] BINENBOJM, Gustavo. O princípio da transparência na Lei Geral de Proteção de Dados. In: SARLET, Ingo Wolfgang; MENEZES, Joyceane Bezerra de; LIMA, Cíntia de Freitas (coords.). LGPD e a Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2020.

A certificação digital, emitida por Autoridades Certificadoras, é uma das principais tecnologias que garantem a autenticidade. Ela cria uma identidade virtual que vincula a chave de criptografia a uma pessoa ou entidade. Quando um ato é assinado digitalmente, é possível verificar a identidade do emissor e comprovar que o documento não foi alterado. Como aponta Marinoni (2015) [36] , essa tecnologia é crucial para manter a segurança jurídica, pois impede que o ato seja falsificado ou que sua autoria seja contestada.

A irretratabilidade, também conhecida como não repúdio, é o princípio que impede que o remetente de uma mensagem negue tê-la enviado ou que o destinatário negue tê-la recebido. Esse é um ponto crucial, especialmente para a validade da citação, que exige a ciência inequívoca do réu sobre a existência do processo.

Para comprovar a entrega e garantir a irretratabilidade, o Processo Judicial Eletrônico utiliza a prova de entrega eletrônica. Os sistemas dos tribunais registram o momento exato em que a citação ou intimação é disponibilizada no sistema do advogado ou da parte. O Código de Processo Civil de 2015 (CPC) determina que as intimações sejam consideradas realizadas na data de sua disponibilização, e que o prazo para a prática do ato processual começa a contar a partir do primeiro dia útil seguinte à sua leitura (BRASIL, 2015) [37] .

No entanto, a confiabilidade da prova de entrega nem sempre é absoluta, principalmente quando se utiliza ferramentas fora dos sistemas oficiais do Judiciário. O Superior Tribunal de Justiça (STJ), em um caso que envolveu a citação por meio de aplicativo de mensagens, validou o ato, mas condicionou sua eficácia à existência de elementos que confirmem a autenticidade e a ciência da parte, como a fotografia de perfil e a confirmação de recebimento (STJ, 2017) [38] . Essa postura cautelosa do Judiciário demonstra que a mera entrega da mensagem não é suficiente: é preciso garantir que o ato foi praticado por quem devia e que chegou a quem devia.

A LGPD, por sua vez, adiciona uma camada de responsabilidade a esse processo. O operador do sistema — o próprio tribunal — tem o dever de adotar "medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações de destruição, perda, alteração, comunicação ou difusão indevida" (BRASIL, 2018) [39] . Assim, a validade

[35] BRASIL. Lei nº 11.419, de 19 de dezembro de 2006. Dispõe sobre a informatização do processo judicial. Diário Oficial da União, Brasília, DF, 20 dez. 2006.
[36] MARINONI, Luiz Guilherme. O Processo Eletrônico: Eficiência sem garantias?. Revista de Processo, v. 240, p. 1-15, 2015.
[37] BRASIL. Lei nº 13.105, de 16 de março de 2015. Código de Processo Civil. Diário Oficial da União, Brasília, DF, 17 mar. 2015.
[38] SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). REsp 1646271/MG. Relator: Ministro Luis Felipe Salomão, Quarta Turma, julgado em 06/06/2017, DJe 08/08/2017
[39] 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

e a irretratabilidade de uma comunicação eletrônica estão intrinsecamente ligadas à capacidade do sistema de garantir a proteção dos dados nela contidos.

6 CONCLUSÕES

A análise detalhada sobre a validade e a segurança jurídica das comunicações processuais eletrônicas à luz da LGPD revelou um cenário de avanço tecnológico, mas também de desafios significativos. A celeridade e a eficiência, impulsionadas pelo processo eletrônico, não podem comprometer os direitos fundamentais à privacidade e à proteção de dados.

O estudo demonstrou que a validade jurídica da citação e da intimação eletrônica, embora respaldada pelo Código de Processo Civil de 2015, está intrinsecamente ligada à segurança dos sistemas que as veiculam. O Processo Judicial Eletrônico, em sua essência, trata uma vasta quantidade de dados pessoais e, como tal, deve se submeter aos princípios da LGPD.

A pesquisa concluiu que, apesar do grande salto tecnológico, ainda existem falhas que podem comprometer a validade jurídica dos atos processuais. Sistemas que não utilizam criptografia adequada, que permitem o acesso por credenciais fracas ou que não oferecem uma prova de entrega infalível, colocam em risco a segurança do processo e, consequentemente, podem levar à anulação dos atos. A colisão entre a busca por eficiência e a proteção de dados não é apenas teórica; ela já se manifesta em decisões judiciais que, por cautela, questionam a validade de comunicações realizadas por meios não oficiais, como no caso da citação via WhatsApp (STJ, 2017) [40] .

A LGPD, portanto, não é um obstáculo à digitalização da justiça, mas um catalisador para que essa modernização ocorra de forma segura e responsável. Conforme ensina Doneda (2019) [41] , a proteção de dados deve ser vista como um princípio estruturante e não como uma mera regra formal. A conformidade não se resume a uma base legal para o tratamento de dados (como o art. 7º, inciso VI da LGPD), mas à observância rigorosa de todos os princípios, em especial o da segurança, necessidade e transparência.

Para superar os desafios identificados, propõe-se uma série de medidas que visam a fortalecer a segurança e a validade jurídica das comunicações eletrônicas, garantindo a conformidade do Poder Judiciário com a LGPD:

Desenvolvimento de Protocolos Mais Rigorosos de Segurança: É imperativo que o Conselho Nacional de Justiça (CNJ) estabeleça e exija a adoção de um padrão mínimo de segurança da informação para todos os sistemas de intimação e citação eletrônica. Tais protocolos devem incluir a

[40] SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). REsp 1646271/MG. Relator: Ministro Luis Felipe Salomão, Quarta Turma, julgado em 06/06/2017, DJe 08/08/2017

[41] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. São Paulo: Editora Revista dos Tribunais, 2019.

obrigatoriedade de uso de criptografia de ponta a ponta, a implementação de autenticação de múltiplos fatores (MFA) e a realização de auditorias de segurança periódicas.

Maior Transparência na Coleta e Tratamento dos Dados: O Poder Judiciário deve criar políticas de privacidade claras e acessíveis, que informem aos titulares de dados (partes e advogados) como suas informações são coletadas, armazenadas e utilizadas. Conforme a LGPD, a transparência é um direito do cidadão e um dever do controlador (BRASIL, 2018) [42] .

Capacitação dos Operadores do Direito e da Sociedade: A segurança não é apenas uma questão técnica, mas também humana. É crucial que magistrados, servidores, advogados e cidadãos sejam capacitados sobre os riscos e as melhores práticas de segurança digital. Uma compreensão aprofundada da LGPD e das ameaças cibernéticas é fundamental para o uso seguro das ferramentas eletrônicas e para a construção de uma cultura de proteção de dados no ambiente judicial.

A implementação dessas propostas é crucial para que a citação e a intimação eletrônica continuem a ser instrumentos eficazes da celeridade processual, sem comprometer a segurança jurídica e a proteção dos direitos fundamentais dos cidadãos no ecossistema digital.

[42] 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

REFERÊNCIAS

BINENBOJM, Gustavo. O princípio da transparência na Lei Geral de Proteção de Dados. In: SARLET, Ingo Wolfgang; MENEZES, Joyceane Bezerra de; LIMA, Cíntia de Freitas (coords.). LGPD e a Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2020.

BRASIL. Lei nº 11.419, de 19 de dezembro de 2006. Dispõe sobre a informatização do processo judicial. Diário Oficial da União, Brasília, DF, 20 dez. 2006.

BRASIL. Lei nº 13.105, de 16 de março de 2015. Código de Processo Civil. Diário Oficial da União, Brasília, DF, 17 mar. 2015.

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.

DIDIER JR., Fredie. Curso de direito processual civil: teoria do processo judicial, processo de conhecimento e procedimento comum. v. 1. Salvador: JusPodivm, 2018.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. São Paulo: Editora Revista dos Tribunais, 2019.

GIL, Antônio Carlos. Como elaborar projetos de pesquisa. 4. ed. São Paulo: Atlas, 2002.

MARINONI, Luiz Guilherme. O Processo Eletrônico: Eficiência sem garantias?. Revista de Processo, v. 240, p. 1-15, 2015.

MINAYO, Maria Cecília de Souza. O desafio do conhecimento: pesquisa qualitativa em saúde. 14. ed. São Paulo: Hucitec, 2014.

SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). REsp 1646271/MG. Relator: Ministro Luis Felipe Salomão, Quarta Turma, julgado em 06/06/2017, DJe 08/08/2017.

TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL (TJRS). Agravo de Instrumento nº 70083547901. 22ª Câmara Cível, julgado em 29/01/2020.