CENTRO UNIVERSITÁRIO DE BRASÍLIA – CEUB
INSTITUTO CEUB DE PESQUISA E DESENVOLVIMENTO – ICPD
PROGRAMA DE MESTRADO EM DIREITO E POLÍTICAS PÚBLICAS

A LEI GERAL DE PROTEÇÃO DE DADOS E O TRATAMENTO DE DADOS PESSOAIS PELO PODER JUDICIÁRIO BRASILEIRO

Brasília/DF
2022

ROSÁRIA FÁTIMA RESENDE BELINATI SALGUEIRO COSTA

A LEI GERAL DE PROTEÇÃO DE DADOS E O TRATAMENTO DE DADOS PESSOAIS PELO PODER JUDICIÁRIO BRASILEIRO

Dissertação apresentada como critério parcial de aprovação no programa de Mestrado em Direito e Políticas Públicas do Centro Universitário de Brasília – CEUB, na área de concentração em Políticas Públicas, Relações Privadas e Desenvolvimento, na linha de pesquisa Políticas Públicas, Sociedade Civil e Proteção da Pessoa.

Orientador: Prof. Dr. Leonardo Roscoe Bessa

Brasília/DF

2022

ROSÁRIA FÁTIMA RESENDE BELINATI SALGUEIRO COSTA

A LEI GERAL DE PROTEÇÃO DE DADOS E O TRATAMENTO DE DADOS PESSOAIS PELO PODER JUDICIÁRIO BRASILEIRO

Dissertação apresentada como critério parcial de aprovação no programa de Mestrado em Direito e Políticas Públicas do Centro Universitário de Brasília – CEUB, na área de concentração em Políticas Públicas, Relações Privadas e Desenvolvimento, na linha de pesquisa Políticas Públicas, Sociedade Civil e Proteção da Pessoa.

BANCA EXAMINADORA

Local: Instituto CEUB de Pesquisa e Desenvolvimento - ICPD
Horário: 11h
Data: 19/12/2022

Prof. Dr. Leonardo Roscoe Bessa
Orientador – CEUB

Prof. Dra. Liziane Paixão Silva Oliveira
Membro Interno – CEUB

Prof. Dr. Diógenes Faria de Carvalho
Membro Externo – UFG

Dedico este trabalho ao meu marido, Paulo Henrique, meu eterno amor. Dedico aos meus filhos, razões da minha existência, Anjinho que está no céu, Juan Diego, João Paulo e todos os filhos que porventura Deus nos agraciar.

AGRADECIMENTOS

A Deus, a quem tudo confio, que sempre esteve ao meu lado, sendo paz ao meu coração. Obrigada Senhor por ter sido minha força em todos os momentos deste trabalho e não ter feito eu desistir. Pelo contrário, a cada obstáculo, me tornava mais forte em continuar. A cada palavra deste trabalho, honro e agradeço a Ti. Sem o Senhor não sou nada, não teria alcançado esse sonho. Toda vitória, tudo que tenho e sou devo a Ti, meu Senhor!

À minha Mãezinha do Céu, Nossa Senhora, que sempre foi minha fonte de amor e cuidado. Ela que me acalmou e abraçou nos momentos mais difíceis e fez com que conseguisse, ao longo desses 4 anos de Mestrado, ainda cumprir com meu papel de serva de Deus, esposa, mãe, filha, irmã, nora, cunhada e amiga.

Ao meu marido, Paulo Henrique, meu eterno amor, por ter me dado colo e força nos momentos mais difíceis, por ter sido meu maior incentivador a alcançar esse tão sonhado Mestrado. Pela paciência, compreensão, amor e cuidado que sempre teve comigo, com o João Paulo na barriguinha da mamãe, me acompanhando em todos os exames de gravidez e em tudo que precisasse, e, principalmente, sendo presença e carinho na vida do nosso filho Juan Diego diante da minha ausência. Tudo isso e muito mais foram fundamentais para minha tranquilidade. Agradeço, ainda, de forma especial, pelos momentos inesquecíveis vividos no decorrer desses 4 anos de mestrado, nosso casamento e três filhos maravilhosos que são bênçãos de Deus em nossas vidas. Viver todos os dias ao seu lado é o maior presente que Deus me deu, minha maior alegria, pois você me completa e me faz querer ser melhor todos os dias. Obrigada por ser esse marido e pai presente e por cuidar tão bem de nossa família. Te Amo!

Aos meus amados filhos, Anjinho no céu, Juan Diego e João Paulo.

Anjinho no céu, meu amor, obrigada por ter intercedido à Deus para que a mamãe conseguisse finalizar o trabalho de Mestrado e por ser essa benção em nossas vidas.

Juan Diego, meu amor, obrigada por ter conseguido lidar, em tão pequena idade, com o sentimento de ausência da mamãe durante os últimos meses de conclusão. Saiba que essa foi a maior dor que senti ao realizar este trabalho. Porém, ver sua evolução, sentir seu amor, carinho e alegria foram meus maiores combustíveis para continuar em frente.

João Paulo, meu amor, você foi o mais privilegiado, pois viveu todo o trabalho escrito do Mestrado dentro da barriguinha da mamãe, acompanhando todas as minhas angústias e vitórias em cada finalização de capítulo. Obrigada por ter vivido tudo isso ao meu lado, sendo força e esperança para a mamãe. Seu nascimento, que será poucos dias após a apresentação do trabalho à banca final, será meu maior presente e vitória.

Meus amados filhos, meu maior desejo é ter conseguido transmitir a vocês a mensagem de que lutar por nossos sonhos vale a pena, mesmo que o caminho pareça árduo, difícil ou, até mesmo, impossível. O que mais me deu força para concluir este trabalho e alcançar esse sonho foi pensar que seria um bom exemplo e força nos momentos mais difíceis e de decisões na vida de vocês. Lutem pelos seus sonhos, voem alto, se caírem, se levantem mais fortes e voem mais alto ainda. Sejam felizes e honrem os dons que Deus deu para cada um. É o que a mamãe mais deseja.

Aos meus amados pais, Roberval e Rosângela, por toda a disponibilidade em ajudar, amor e incentivo durante toda a minha caminhada, por continuarem sendo o meu alicerce e meus maiores exemplos de luta e vitória profissional. Toda a minha gratidão por, desde tão nova, terem me incentivado a fazer o curso de Direito, oferecendo, até hoje, tudo que podem para meu crescimento e realização profissional. Tudo que sou, devo a vocês. Meu eterno agradecimento e amor.

Aos meus irmãos amados, minhas cunhadas e cunhado, Rober, Rosana e Rener, Roberlan e Kamilla, Roberlei e Nathália, e Rôberson, todos colegas de profissão, que sempre apoiaram meus sonhos, que trouxeram vários momentos alegres e descontraídos durante essa fase, tornando-a mais leve e tranquila. As lutas e vitórias de cada um na nossa profissão são grandes exemplos e incentivos para mim.

Um agradecimento especial aos meus irmãos Roberlan, Roberlei e cunhada Nathália, que foram essenciais na decisão de iniciar o mestrado, inclusive, sendo meus colegas de sala de aula, tornando o curso mais alegre e tranquilo. Saibam que foram meus maiores apoiadores a não desistir. Nos momentos mais difíceis me confortaram com palavras de incentivo, reacendendo a chama e vontade de continuar em frente até o final. Muito obrigada!

À família do meu marido, meus amados sogros e cunhado, Glória Christina, Ecidelmon e Vinícius, que foram anjos da guarda em todo o período de escrita deste trabalho, cuidando tão bem da nossa família, principalmente do nosso pequeno Juan Diego. Trouxeram mais alegria à nossa casa e tranquilidade ao meu coração em saber que minha casa e filho estavam sendo muito bem cuidados por vocês. Serei eternamente grata pelo carinho, cuidado e amor que tiveram conosco. Sem vocês, não teria conseguido finalizar este trabalho. Minha eterna gratidão!

Aos meus amados avós que estão no céu, José e Cidinha, que nos momentos mais difíceis deste trabalho foram a quem mais recorri pela intercessão divina. Tenho certeza que estão muito felizes e orgulhosos no céu com a conclusão desta pesquisa.

Ao meu orientador, Professor Doutor Leonardo Roscoe Bessa, por seu estímulo e disponibilidade ao longo desta pesquisa, pela paciência em aceitar as mudanças de tema e firmeza em conduzi-las e, principalmente, por ter me apoiado a não desistir nos momentos de dificuldade pessoais. Tive a honra de ser orientada pelo professor que, por meio de grupos de pesquisa e aulas instigantes e de notável saber, despertou em mim o desejo de continuar os estudos na área de Proteção de Dados Pessoais/LGPD, dominada com maestria pelo excepcional jurista que é.

Aos demais professores da banca, Dr. Diógenes e Dra. Liziane, que na minha qualificação, com muito carinho e atenção, deram conselhos valiosos para a melhoria do meu trabalho e foram luz no meu caminho, juntamente com meu professor orientador, para que conseguisse desenvolver um trabalho de grande valia para a área acadêmica, para o Poder Judiciário e, principalmente para a proteção dos dados pessoais dos cidadãos, visando a garantia dos direitos fundamentais que envolvem a dignidade da pessoa humana, como os direitos à privacidade e intimidade.

"Posso, tudo posso Naquele que me fortalece. Nada e ninguém no mundo vai me fazer desistir.
Quero, tudo quero, sem medo entregar meus projetos, deixar-me guiar nos caminhos que Deus desejou pra mim e ali estar.
Vou perseguir tudo aquilo que Deus já escolheu pra mim.
Vou persistir, e mesmo nas marcas daquela dor do que ficou, vou me lembrar.
E realizar o sonho mais lindo que Deus sonhou. Em meu lugar estar na espera de um novo que vai chegar
Vou persistir, continuar a esperar e crer
E mesmo quando a visão se turva e o coração só chora
Mas na alma, há certeza da vitória"
(Celina Borges e Pe. Fábio de Melo)

RESUMO

O sistema judiciário do Brasil instituiu o Processo Judicial Eletrônico (PJe) e o Diário de Justiça Eletrônico (DJe), que vêm promovendo grandes mudanças em todo o ecossistema do judiciário. Essas mudanças buscam aumentar a celeridade processual, reduzir custos e facilitar o acesso à justiça. Por outro lado, o sistema tem o potencial de, ao alcance de um clique, expor a privacidade e intimidade das partes, colocado em risco seus dados pessoais. A presente dissertação investiga a exposição de dados pessoais, tanto no Processo Judicial Eletrônico, como no Diário de Justiça Eletrônico. Investiga se as medidas adotadas pelo Judiciário Brasileiro no tratamento de dados pessoais estão em consonância com as normas previstas pela Lei Geral de Proteção de Dados Pessoais – Lei 13.709/2018, assim como os desafios enfrentados para essa adequação. Nesse sentido, não só em virtude da Lei Geral de Proteção de Dados Pessoais - LGPD, mas também pautado em outros princípios constitucionais, são propostos modelos de Pseudonimização para os dados pessoais expostos nas decisões judiciais e jurisprudência e da Autodeterminação Informativa do titular do dado como forma de aplicar, automaticamente, o instituto do segredo de justiça a todo e qualquer dado e documento pessoal presente em um processo judicial eletrônico. Os modelos apresentados não ferem o direito fundamental da publicidade dos atos processuais, e sim, dão mais efetividade às normas da LGPD, resguardando os direitos fundamentais da privacidade e intimidade das partes no processo judicial eletrônico. A metodologia utilizada para o desenvolvimento deste trabalho foi a pesquisa bibliográfica, a análise de legislações, da doutrina, de artigos acadêmicos, jurisprudência e estudos feitos pelo Comitê de Proteção de Dados Pessoais do Conselho Nacional de Justiça (CNJ).

Palavras-chave: Lei Geral de Proteção de Dados Pessoais – Lei 13.709/2018. Tratamento de dados pessoais. Processo Judicial Eletrônico. Pseudonimização. Autodeterminação Informativa. Segredo de Justiça.

ABSTRACT

The judiciary system in Brazil instituted the Electronic Judicial Process (PJe) and the Electronic Justice Diary (DJe), which have been promoting major changes throughout the judiciary ecosystem. These changes seek to increase procedural speed, reduce costs and facilitate access to justice. On the other hand, the system has the potential, at the click of a button, to expose the privacy and intimacy of the parties, putting their personal data at risk. The present study investigates the exposure of personal data both in the Electronic Judicial Process and in the Electronic Justice Diary. It investigates whether the measures adopted by the Brazilian Judiciary in the processing of personal data are being effective in complying with the rules provided for by the General Law for the Protection of Personal Data - Law 13.709/2018, as well as the challenges faced for this adequacy. In this sense, not only by virtue of the General Law for the Protection of Personal Data (LGPD), but also based on other constitutional principles, Pseudonymization models are proposed for the personal data exposed in court decisions and jurisprudence and Informative Self-Determination of the data subject as way of automatically applying the institute of secrecy of justice to any and all personal data present in an electronic judicial process. The models presented do not violate the fundamental right of publicity of procedural acts, but rather protect the privacy and intimacy of the parties in the electronic process, and give effect to the rules of the LGPD.

Keywords: General Personal Data Protection Law – Law 13.709/2018. Processing of personal data. Electronic Judicial Process. Pseudonymization. Informative self-determination. Justice secret.

SUMÁRIO

1 INTRODUÇÃO

As profundas transformações sociais causadas pela evolução das tecnologias de armazenamento, compartilhamento e processamento de dados fizeram surgir a Lei Geral de Proteção de Dados Pessoais como uma resposta do ordenamento jurídico brasileiro. A disseminação do uso de sistemas computacionais como suporte preferencial da informação (em substituição ao papel), a consagração da rede mundial de computadores como via de intercâmbio de dados e a proliferação de tecnologias cada vez mais eficientes de recuperação da informação e de mineração e análise massiva de dados são alguns dos fenômenos que deram causa ao recente processo (ainda em andamento) de reformulação do arcabouço jurídico de proteção dos dados de pessoas naturais[1].

Especificamente no âmbito do Poder Judiciário, a transformação digital tem se concretizado paulatinamente, desde os anos 1990, a partir das evoluções tecnológicas, como, por exemplo, a criação de ferramentas públicas de pesquisa textual em repositórios de jurisprudência, o fornecimento de informações sobre andamentos processuais pela internet, a divulgação dos diários de justiça pela rede mundial de computadores, a concessão de acesso público aos autos processuais por meio eletrônico, a instituição da política de dados abertos em bases judiciais e o consumo massivo de dados dos tribunais por terceiros com intuito comercial, por exemplo. É certo que essas e outras medidas voltadas à ampliação do acesso a informações judiciais extraem seu fundamento de validade diretamente da Constituição Federal, que atribui à administração pública o dever de observar o princípio da publicidade (art. 37, caput), determina que todos os julgamentos dos órgãos do Poder Judiciário sejam públicos (art. 93, IX) e prescreve a publicidade dos atos processuais como regra (art. 5º, LX)[2].

Por meio da Lei nº 11.419, de 19 de dezembro de 2006, instituiu-se o Processo Judicial Eletrônico (PJe) e o Diário de justiça Eletrônico (DJe) que vêm promovendo mudanças profundas em todo o ecossistema judiciário brasileiro, com o objetivo de melhorar a qualidade dos serviços judiciais entregue aos cidadãos, como mais celeridade na tramitação processual e acesso à justiça, compreendendo advogados, magistrados, serventuários, membros do Ministério Público, partes, e com profundos reflexos na

[1] CONSELHO NACIONAL DE JUSTIÇA. Tratamento de dados pessoais na consulta de jurisprudência: desafio e perspectivas. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2022/02/tratamento-dados-pessoais-consulta-jurisprudencia30-11-21.pdf. Acesso em 29 nov. 2022.
[2] CONSELHO NACIONAL DE JUSTIÇA. Tratamento de dados pessoais na consulta de jurisprudência: desafio e perspectivas.

sociedade. Ainda neste caminhar, processos em meio físico (até então guardados em depósitos) estão passando pelo processo de digitalização, sendo convertidos em dados e metadados, tudo acessível à distância de alguns cliques.

Segundo dados do Conselho Nacional de Justiça (CNJ), disponível no relatório analítico "Justiça em números 2022", ano-base 2021, o Poder Judiciário terminou em 2021 com 62 milhões de ações judiciais em andamento, que é a diferença entre os 77,3 milhões de processos em tramitação e os 15,3 milhões (19,8%) sobrestados ou em arquivo provisório, aguardando definição jurídica futura. Dos 90 órgãos do Judiciário, 44 aderiram integralmente ao Juízo 100% digital, o que abrange 67,7% das serventias judiciais[3]. Em Brasília, no Tribunal de Justiça do Distrito Federal e dos Territórios (TJDFT), 100% das Unidades Judiciárias de 1° e 2º grau, Turmas Recursais, Unidade de apoio direto às Unidades Judiciárias e o Cartório Judicial Único já operam no PJe[4].

Diante dos dados obtidos pelo CNJ, é possível afirmar que o Poder Judiciário é um dos órgãos públicos que mais coleta e armazena dados pessoais. Os processos judiciais são uma fonte inesgotável de dados pessoais, principalmente dados sensíveis, titularizados pelos mais variados atores processuais (partes, testemunhas, vítimas, magistrados(as), advogados(as), auxiliares da justiça etc.) e terceiros. Qualquer discussão equilibrada sobre a publicidade de atos processuais, nos dias atuais, deve necessariamente considerar o fato de que as ferramentas tecnológicas hoje disponíveis amplificaram, de modo exponencial, a capacidade de armazenamento, compartilhamento e processamento das informações judiciais, inclusive para fins maliciosos e antijurídicos. Por isso que no atual estágio de desenvolvimento tecnológico, já não é mais possível afirmar a irrestrita publicidade de informações judiciais sem levar em consideração os riscos concretos que ela pode oferecer aos direitos da personalidade, imagem, honra, reputação, privacidade, entre outros direitos fundamentais garantidos constitucionalmente.

Nesse contexto, o problema central do presente trabalho diz respeito aos riscos à privacidade e intimidade das partes processuais, em razão de seus dados pessoais estarem cada vez mais expostos na rede mundial de computadores pelos processos judiciais

---

[3] CONSELHO NACIONAL DE JUSTIÇA. Justiça em Números 2022: Judiciário julgou 26,9 milhões de processos em 2021. Disponível em https://www.cnj.jus.br/justica-em-numeros-2022-judiciario-julgou-269-milhoes-de-processos-em-2021/#:~:text=Justi%C3%A7a%20em%20N%C3%BAmeros%202022%3A%20Judici%C3%A1rio,processos%20em%202021%20%2D%20Portal%20CNJ&text=O%20Poder%20Judici%C3%A1rio%20concluiu%2026,solucionados%20em%20rela%C3%A7%C3%A3o%20a%202020. Acesso em: 21 nov. 2022.

[4] TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E TERRITÓRIOS. Aqui tem PjE. Disponível em: https://www.tjdft.jus.br/pje/aqui-tem-pje. Acessado em 9. Dez 2022.

eletrônicos, e disponíveis a todos os advogados e demais membros do judiciário cadastrados no PJE, que não possuem nenhum vínculo direto ao processo e às partes, com exceção aos processos que tramitam em segredo de justiça.

Segundo o site oficial da OAB, o Brasil é o país com a maior proporção de advogados por habitante do mundo. Ao todo, cerca de 1,3 milhão de advogados exercem regularmente a profissão entre 212,7 milhões de pessoas (IBGE). Proporcionalmente, há 1 advogado para 164 brasileiros residentes no país[5], o que é possível questionar diante de tal proporção se realmente são necessários todos os advogados e demais membros do judiciário, que não possuem nenhum vínculo direto ao processo, terem acesso livre aos dados e documentos pessoais das partes em um processo judicial eletrônico.

Ao longo do trabalho será discutida essa questão, porém, é possível adiantar que o acesso livre de advogados, demais membros do judiciário e terceiros aos milhões de dados e documentos pessoais das partes presentes em processos judiciais eletrônicos, com exceção dos processos que tramitam em segredo de justiça, gera às partes perda no controle de seus dados, tornando-as vulneráveis a terem sua privacidade e intimidade violadas através de vazamentos, compartilhamentos ilegais e utilização de seus dados para outras finalidades.

Diante dessa realidade, a pesquisa tem como objetivo principal estudar o tratamento de dados pessoais realizado pelo Poder Judiciário e analisar se estão de acordo com as normas previstas na Lei Geral de Proteção de Dados (LGPD), Lei 13.709/2018, que garantem a proteção dos dados pessoais dos cidadãos e o livre desenvolvimento da personalidade e a dignidade da pessoa humana.

Assim, questiona-se, como tema-problema: o tratamento de dados pessoais realizado pelo Poder Judiciário nos processos judiciais eletrônicos está sendo efetivo conforme as normas da LGPD, respeitando os direitos fundamentais da privacidade e intimidade das partes?

Desse modo, o objetivo geral do trabalho foi propor métodos de aprimoramento ao PJe e DJe de modo a resguardar o cidadão contra o uso abusivo e indiscriminado dos seus dados pessoais. Já os objetivos específicos foram: (b) analisar o processo judicial eletrônico brasileiro, cotejando-o com os direitos fundamentais da publicidade e da

[5] ORDEM DOS ADVOGADOS DO BRASIL. Brasil tem 1 advogado a cada 164 habitantes; CFOAB se preocupa com qualidade dos cursos jurídicos. Disponível em: https://www.oab.org.br/noticia/59992/brasil-tem-1-advogado-a-cada-164-habitantes-cfoab-se-preocupa-com-qualidade-dos-cursos-juridicos. Acessado em 25 nov. 2022.

privacidade; (c) realizar a ponderação e otimização dos princípios da publicidade e da privacidade; (d) identificar o objetivo, fundamentos e princípios que regem a LGPD e sua incidência no âmbito do Poder Judiciário brasileiro, em especial, no âmbito do processo judicial eletrônico, no tocante ao tratamento de dados pessoais dos litigantes; (e) verificar a adequação do Judiciário brasileiro à LGPD, mediante um paralelo com o tratamento de dados pessoais, empregados por países estrangeiros, e as consequências práticas do agir tecnológico judicial brasileiro, analisando, ao final, a possibilidade da implantação dos métodos da pseudonimização dos dados pessoais dos litigantes nas decisões judiciais e jurisprudência e da Autodeterminação Informativa como forma do titular do dado aplicar, automaticamente, o instituto do segredo de justiça em qualquer dado e documento pessoal presente no processo judicial eletrônico, retirando essa autonomia do magistrado.

Nesse sentido, o desenvolvimento do trabalho estrutura-se em três capítulos. O primeiro capítulo tem como objetivo apresentar uma parte histórica sobre a evolução do tema proteção de dados pessoais na União Europeia, como no ordenamento jurídico brasileiro, até chegar à Lei de Proteção de Dados Pessoais – Lei 13.709/2018. O objetivo de trazer essa evolução das normas que garantem a proteção dos dados pessoais é para demonstrar como a proteção dos dados pessoais se tornou um ativo de tamanha importância nos dias atuais, de modo que sua proteção é fundamental e de interesse não apenas dos titulares dos dados, mas de toda a sociedade.

Após a parte histórica, foram apresentados conceitos importantes da LGPD que serviram como base para os demais capítulos, referente ao tratamento de dados pessoais pelo Poder Público, como a parte principiológica prevista no art. 6º, da lei, como o da transparência, segurança, prevenção e responsabilização e prestação de contas, e as bases legais previstas nos arts. 7º e 11º que servem como justificativa para o tratamento de dados pessoais e sensíveis, como o Consentimento Informado, o Cumprimento de Obrigação Legal ou Regulatória pelo Controlador, a Execução de políticas públicas pela Administração Pública, o Exercício regular de direitos em processo judicial e o Legítimo Interesse.

No segundo capítulo foram apresentados os desafios enfrentados pelo Poder Judiciário na proteção de dados pessoais sob as normas da LGPD, como a colisão dos direitos fundamentais da publicidade dos atos processuais, privacidade, intimidade e proteção de dados pessoais; a legitimidade do Poder Judiciário em aplicar as normas previstas na LGPD; se os dados coletados e armazenados pelos órgãos do judiciário são passíveis de regulação e estão bem protegidos conforme as normas da lei; se as resoluções

do CNJ que preveem a melhor adequação dos tribunais à LGPD estão de acordo com o objetivo central da lei; a exposição dos dados pessoais e o livre acesso pelos advogados, terceiros e demais membros do judiciário, que não estão vinculados ao processo judicial; a falha do sistema de segurança; ataques frequentes de *hackers* aos sistemas do judiciário; e compartilhamento de dados pessoais.

No terceiro capítulo foram apresentadas as perspectivas de tratamento de dados pessoais pelo Poder Judiciário, no intuito de trazer mais efetividade às normas da LGPD, o que inclui: as prerrogativas e obrigações que devem ser seguidas pelos tribunais seguindo os princípios trazidos pelo art. 6º da lei, as bases legais dos arts. 7º e 11º e demais normas que preveem o tratamento de dados pessoais pelo Poder Público; a fiscalização e aplicação de sanções mais severas da Autoridade Nacional de Proteção de Dados (ANPD) ao Poder Público; a responsabilidade civil objetiva do Poder Público/Judiciário em responder pelos atos e danos causados a terceiros; métodos de restrição ao acesso de dados pessoais por terceiros não vinculados ao processo judicial eletrônico, como o da Pseudonimização nos dados pessoais expostos nas decisões judiciais, jurisprudência e demais serviços de divulgação desses dados; e da Autodeterminação Informativa como forma do titular do dado ter autonomia para aplicar, automaticamente, o instituto do segredo de justiça a qualquer dado e documento pessoal presente no processo judicial eletrônico em que for parte, retirando essa autonomia do magistrado.

A metodologia utilizada para o desenvolvimento do presente trabalho foi a pesquisa bibliográfica, a análise de legislações correlatas ao tema com foco na Lei Geral de Proteção de Dados Pessoais, Lei do Processo Eletrônico, Resoluções Normativas do CNJ criadas para os Tribunais se adequarem às normas da LGPD, da doutrina com destaque aos autores Bruno Bioni, Danilo Doneda, Laura Schertel Mendes, Ricardo Villas Bôas Cueva, de artigos acadêmicos sobre o assunto, jurisprudência, e estudos feitos pelo Comitê de Proteção de Dados Pessoais do Conselho Nacional de Justiça (CNJ).

Apresentadas essas considerações introdutórias, dar-se-á prosseguimento ao desenvolvimento do presente trabalho, com vistas ao aprofundamento do estudo sobre a evolução da proteção de dados pessoais no ordenamento jurídico brasileiro.

2 ASPECTOS GERAIS DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

Diante do atual cenário do mundo que é caracterizado pela era de uma sociedade da informação, o dado pessoal se tornou um ativo de extrema relevância e sua proteção é um dos temas mais debatidos nos dias atuais, tanto pela sociedade, quanto para o ordenamento jurídico. O primeiro capítulo tem como objetivo apresentar uma parte histórica sobre a evolução do tema proteção de dados pessoais na União Europeia, como no ordenamento jurídico brasileiro, até chegar à Lei de Proteção de Dados Pessoais – Lei 13.709/2018. O objetivo de trazer essa evolução das normas que garantem a proteção dos dados pessoais é para demonstrar como a proteção dos dados pessoais se tornou um ativo de tamanha importância nos dias atuais, de modo que sua proteção é fundamental e de interesse não apenas dos titulares dos dados, mas de toda a sociedade.

Após a parte histórica serão apresentados conceitos importantes da LGPD referentes ao tratamento de dados pessoais, como a parte principiológica prevista no art. 6º da lei, como o da transparência, segurança, prevenção e responsabilização e prestação de contas, e as bases legais previstas nos arts. 7º e 11º que servem como justificativa para o tratamento de dados pessoais e sensíveis, como o Consentimento Informado, o Cumprimento de Obrigação Legal ou Regulatória pelo Controlador, a Execução de políticas públicas pela Administração Pública, o Exercício regular de direitos em processo judicial e o Legítimo Interesse, conceitos importantes que serão base para o tratamento de dados pessoais pelo Poder Público, o que inclui o Poder Judiciário, e para os próximos capítulos.

2.1 DA EVOLUÇÃO DAS REGULAMENTAÇÕES DE PROTEÇÃO DE DADOS PESSOAIS NA UNIÃO EUROPEIA E NO ORDENAMENTO JURÍDICO BRASILEIRO

Os primeiros países que subscreveram declarações a respeito do direito à privacidade e proteção de dados foram países europeus por meio da Declaração da ONU

de Direitos Humanos (1948)[6] e Declaração Europeia dos Direitos do Homem (1950)[7], porém, a proteção de dados pessoais era tratada de maneira vaga e superficial.

Após, veio a Convenção nº 108 do Conselho da Europa[8] que estabeleceu a proteção de indivíduos quanto ao processamento automático de tratamento de dados, o que objetivou instituir métodos mais criteriosos como a previsão das "garantias relativas à coleta e tratamento de dados pessoais", e proibiu "na ausência de garantias jurídicas adequadas, o tratamento de dados sensíveis, tais como dados sobre a raça, a opinião política, a saúde, as convicções religiosas, a vida sexual ou o registro criminal de uma pessoa".

Contudo, em 1995, a União Europeia, ainda não satisfeita, sentiu necessidade de aperfeiçoar e dar efetividade à Convenção nº 108 e promulgou a Diretiva nº 95/46/CE[9], que pretendia estabelecer, harmonizar e promover igualdade no tratamento de dados pessoais pelos Estados-Membros. Por se tratar de uma diretiva, seria necessário que cada Estado adotasse o texto comunitário em seu direito interno, o que ensejou diferentes níveis de proteção em cada um dos países europeus. No entanto, essa Diretiva (Regulamento Geral sobre a Proteção de Dados) foi revogada pelo Parlamento Europeu e do Conselho[10], sob o Regulamento (UE) nº 2.016/679, que trata da proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Dois anos mais tarde, entrou em vigor uma das leis mais importantes que trata da proteção de dados pessoais, em nível internacional, que serve de modelo para vários países do mundo, que é o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia, com 11 capítulos e 99 artigos. O referido regulamento atualizou, harmonizou e adaptou a antiga Diretiva Europeia de Proteção de Dados às mais novas formas de uso massivo de dados pessoais, tais como os modelos de negócio baseados em tecnologias de big data, inteligência artificial e aprendizado de máquina. O regulamento estabelecia as

---

[6] NAÇÕES UNIDAS BRASIL. Os Objetivos de Desenvolvimento Sustentável no Brasil. Disponível em: https://nacoesunidas.org/direitoshumanos/declaracao/. Acesso em: 01 set. 2022.

[7] UNIÃO EUROPEIA. Convenção Europeia dos Direitos dos Homens. Disponível em: https://www.echr.coe.int/Documents/Convention_POR.pdf. Acesso em: 01 set. 2022.

[8] UNIÃO EUROPEIA. Council of Europe. Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37. Acesso em: 01 set. 2022.

[9] UNIÃO EUROPEIA. Directiva 95/46/CE do Parlamento Europeu e do Conselho. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 01 set. 2022.

[10] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679. Acesso em: 01 set. 2022.

regras relativas ao tratamento, por uma pessoa, uma empresa ou uma organização de dados pessoais relativos a pessoas.

Na GDPR, nos artigos 4º, itens 13, 14 e 15, e 9, além dos Considerandos 51 a 56, há previsão sobre os denominados dados sensíveis, que são os dados pessoais que revelem origem racial ou étnica, opiniões políticas e convicções religiosas ou filosóficas; filiação sindical; dados genéticos, dados biométricos tratados simplesmente para identificar um ser humano; dados relacionados com a saúde; dados relativos à vida sexual ou orientação sexual da pessoa. O artigo 4º, itens 2 e 6, da GDPR, inclui como sendo o tratamento de dados, o recolhimento, o registro, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, comparação ou interconexão, limitação, o pagamento ou a destruição de dados pessoais.

Na Alemanha, pode-se citar a Lei Federal de Proteção de Dados de 2017 (Bundesdatenschutzgesetz – BDSG)[11], que segue os preceitos da GDPR e pretendeu substituir a lei de mesmo nome que havia sido instituída em 2001. A BDSG trata dos direitos e deveres de órgãos públicos e privados para as atividades de coleta e processamento de dados, que têm o dever de contratar um profissional responsável por privacidade de dados e de determinar regras claras para avaliações de *score* de crédito, por exemplo. Além disso, há diretrizes específicas para como as empresas devem e podem fazer tratamentos de dados de seus funcionários.

É nesse contexto que as leis de proteção de dados pessoais, editadas por diversos países e blocos econômicos mundiais, cumpriram o papel de conter o descontrole do tratamento de informações por agentes públicos e privados, que, diante de leis específicas, devem, agora, observar, prioritariamente, os interesses dos indivíduos, titulares de dados pessoais e da legitimidade da circulação de informações. Diante da inviabilidade de se conter ou suprimir a circulação de dados numa sociedade marcada pela necessidade de desenvolvimento econômico, as leis de proteção de dados, editadas de forma quase mundial, não tiveram o objetivo de impedir o tratamento de dados, mas sim de regular a circulação de informações pessoais. Já em relação ao ordenamento jurídico brasileiro, embora o Brasil não houvesse sido o precursor da discussão sobre tratamento e proteção de dados pessoais, no âmbito digital ou físico, a matéria já era positivada de forma indireta no ordenamento jurídico brasileiro no art. 5º, X, da Constituição da República Federativa

[11] Disponível em: https://www.gesetze-im-internet.de/bdsg_2018/. Acesso em: 01 set. 2022.

do Brasil, de 1988, ao dispor sobre a inviolabilidade da intimidade, da vida privada, da honra e da imagem dos cidadãos.

Para isso, se faz necessário analisar as iniciativas legislativas anteriores que versaram sobre o direito à privacidade e que mencionam superficialmente sobre a proteção desses dados. Será possível perceber que o legislador sempre teve uma preocupação no que tange à proteção da informação pessoal, ainda que as legislações analisadas não tratem objetiva e diretamente sobre o assunto. Assim, no plano infraconstitucional brasileiro, o direito à privacidade recebeu tutela pelo art. 21 da Lei nº 10.406, de 10 de janeiro de 2002 – Código Civil, pelo art. 11 da Lei nº 8.078, de 11 de setembro de 1990 – Código de Defesa do Consumidor, pela Lei nº 12.414, de 9 de junho de 2011 – Lei de Acesso à Informação e pela Lei nº 12.965, de 23 de abril de 2014 – denominada Marco Civil da Internet, que além de regulamentar o uso da *Internet* no país, trouxe os primeiros parâmetros de autodeterminação informativa e a noção de restringibilidade de circulação de dados pessoais.

Por mais que as referidas normas não citam diretamente sobre proteção de dados pessoais, a Constituição da República Federativa do Brasil traz no caput do art. 5º a proteção à segurança de brasileiros e estrangeiros residentes no país, sendo possível incluir nesse conceito a proteção de dados, além de considerar os direitos fundamentais sob uma ótica expansionista.

O inciso X do referido artigo dispõe que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação"[12]. Já no trecho citado, é possível afirmar que o legislador, ao tratar do direito à privacidade, tratou diretamente da proteção de dados. Já no inciso LX, do mesmo artigo[13], o legislador foi mais específico em tratar da proteção dos dados: "Art 5º, LX, da CF – "a lei só poderá restringir a publicidade dos atos processuais quando a defesa da intimidade ou o interesse social o exigirem".

Já em análise ao Código de Defesa do Consumidor, o objetivo da lei é instaurar direitos e deveres com o intuito de proteger os consumidores, parte hipossuficiente nas relações de consumo. Os artigos 43 e 44 do CDC, aos quais estabelecem algumas regras que visam a proteção e a integridade das informações pessoais dos consumidores, onde

---

[12] BRASIL. *Constituição da República Federativa do Brasil*. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 05 set. 2022.

[13] BRASIL. *Constituição da República Federativa do Brasil*. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 05 set. 2022.

os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podem conter informações negativas referentes a período superior a cinco anos. Em caso de abertura de cadastro, ficha, registro e dados pessoais e de consumo não solicitados pelo consumidor, a lei prevê a obrigatoriedade de autorização por escrito[14]. Também prevê que o consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir imediata correção e deve o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.

Desse modo, por mais que o CDC seja uma lei de referência no assunto, é possível afirmar que o CDC versa sobre a integridade das informações pessoais no âmbito das relações de consumo e não traz muitos elementos que permitem concluir por um direito autônomo à proteção de dados pessoais, o que faz limitar a tutela desse direito[15]. Por outro lado, a Lei de Acesso a Informação – LAI, apesar de versar sobre a publicidade das informações pessoais e de interesse coletivo referente aos órgãos públicos, conceitua em seu art. 4º a informação pessoal como aquela relacionada à pessoa natural identificada ou identificável, de modo que apresenta semelhanças ao disposto na LGPD. O art. 6º, III, da LAI também disciplina sobre a proteção da informação pessoal[16].

Logo adiante, na sessão V, art. 31, a LAI traz disposições expressas sobre as informações pessoais e deixa claro que seu tratamento deve ser transparente e respeitar a intimidade, vida privada, honra e imagem dos seus titulares, bem como as liberdades e garantias individuais[17]. Todavia, Francoski ressalva que tais disposições se mostram

---

[14] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. São Paulo: Thomson Reuters, 2019. p. 265-266.

[15] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. São Paulo: Thomson Reuters, 2019. p. 265-266.

[16] Art. 6º. Cabe aos órgãos e entidades do poder público, observadas as normas e procedimentos específicos aplicáveis, assegurar a: III - proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso.

[17] Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.
§ 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:
I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e
II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.
§ 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido.
§ 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias:

insuficientes ao considerar o avanço tecnológico da sociedade da informação, de modo que a LAI atualmente merece ser interpretada sob o prisma da LGPD.[18]

Quanto ao Marco Civil da Internet, vislumbra-se que a proteção da privacidade e dos dados pessoais se inserem como pilares, ao lado da neutralidade de rede e da liberdade de expressão, conforme dispõe o art. 3º, desta lei[19][20]. A legislação em comento, mais precisamente o capítulo II, art. 7º, VII, IX e art. 16º, II, versa sobre a necessidade do consentimento livre, expresso e informado para coleta, uso, armazenamento e tratamento de dados pessoais, bem como para a transferência desses dados para terceiros[21]. Portanto, a autodeterminação informacional foi prestigiada por essa lei, eis que garante ao titular do dado o controle do fluxo de suas informações pessoais[22].

Portanto, diante das normas apresentadas, é possível ver a evolução no ordenamento jurídico brasileiro sobre o tema, mesmo tratando de forma implícita a proteção de dados pessoais, assim como é possível afirmar que essa evolução contribuiu para os legisladores verem a necessidade de criação de uma lei que dispunha de um instrumento legal que garantisse a efetividade da proteção de dados pessoais com a instituição de órgãos reguladores específicos. Nesse contexto, em 14 de agosto de 2018, foi promulgada a Lei n. 13.709 – Lei Geral de Proteção de Dados Pessoais – LGPD, que

---

I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;
II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;
III - ao cumprimento de ordem judicial;
IV - à defesa de direitos humanos; ou
V - à proteção do interesse público e geral preponderante.
§ 4º A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância.
§ 5º Regulamento disporá sobre os procedimentos para tratamento de informação pessoal.

[18] FRANCOSKI, Denise; TASSO, Fernando. Capítulo 14. O Compartilhamento de Dados Pessoais Oriundos de Bases de Dados Públicas: A Compatibilidade Entre a LAI e a LGPD. *In*: FRANCOSKI, Denise; TASSO, Fernando. *A Lei Geral de Proteção de Dados Pessoais: Lgpd*. Ed. 2021. São Paulo (SP): Editora Revista dos Tribunais. 2021. Disponível em: https://thomsonreuters.jusbrasil.com.br/doutrina/1279975732/a-lei-geral-de-protecao-de-dados-pessoais-lgpd-ed-2021. Acesso em: 05 set. 2022.

[19] Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei; IV - preservação e garantia da neutralidade de rede;

[20] BIONI, Bruno Ricardo. *Proteção de Dados Pessoais*: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021. p. 214.

[21] BIONI, Bruno Ricardo. *Proteção de Dados Pessoais*: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021. p. 214.

[22] BIONI, Bruno Ricardo. *Proteção de Dados Pessoais*: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021. p. 215.

deu origem a um marco legal brasileiro que trata diretamente sobre o tema e que gera impacto para as instituições públicas e privadas. Antes de adentrar nos conceitos de tratamento de dados previstos na lei, necessário se faz abordar um contexto histórico sobre a origem da LGPD.

A Lei Geral de Proteção de Dados Pessoais teve grande contribuição dos debates realizados pelos membros dos países do Mercosul com o intuito de trazer a proteção de dados regulamentada de forma unificada para todos os países membros. Porém, o documento[23] desses debates no Mercosul não resultou em deliberação. Contudo, essas discussões se expandiram ao Ministério da Justiça até a consolidação do anteprojeto, que foi encaminhado à Presidência da República e, posteriormente, à Câmara dos Deputados, e tramitou como Projeto de Lei (PL) n. 5.276/2016[24].

Durante o processo de tramitação legislativa na Câmara, houve o apensamento ao PL n. 4.060/2012[25], além da criação de uma Comissão Especial para tratar do assunto, que contou com intensa participação de diversos setores da sociedade. Quanto à tramitação no Senado Federal, o projeto enviado pela Câmara foi aprovado. O Presidente da República, no que tange à sanção, vetou alguns dispositivos, entre eles o da Autoridade Nacional de Proteção de Dados (ANPD). Posteriormente, foi editada a MP n. 869/2018[26], convertida na Lei n. 13.853/2019[27], que tratou sobre a estrutura da ANPD e sobre *vacatio legis* da LGPD para agosto de 2020[28]. Durante o processo legislativo, houve participação de várias entidades da Sociedade Civil, por meio das audiências públicas realizadas na Câmara dos Deputados e no Senado Federal, como destacado por Bataglia, Lemos e

[23] Versão disponível em: https://documentos.mercosur.int/simfiles/proynormativas/24606_SGT13_2010_ACTA01_ANE04_PDecS-N_ES_Protecci%C3%B3n%20Datos%20Personales.pdf. Acesso em: 21 ago. 2021.

[24] Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378. Acesso em: 21 ago. 2021.

[25] Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066. Acesso em: 21 ago. 2021.

[26] BRASIL. Medida Provisória nº 869, de 27 de dezembro de 2018. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869.htm. Acesso em: 21 ago. 2021.

[27] BRASIL. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF: Presidência da República, [2019]. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm. Acesso em: 21 ago. 2021.

[28] DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. *In*: DONEDA, Danilo et al. (org.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. p. 15-18.

Farranha, no artigo "Proteção de Dados Pessoais e Acesso à Informação: Interfaces do Papel da Sociedade Civil no Processo Legislativo Brasileiro"[29].

É importante destacar que, além da LGPD, existem outros projetos de lei que estão em discussão sobre privacidade e proteção de dados, conforme demostra o estudo realizado pelo Observatório do Data Privacy Brasil, publicado recentemente em seu site[30], o que demonstra que o Brasil passou por um longo caminho para regulamentar de fato a proteção de dados e deverá constantemente aprimorar as legislações já existentes, diante dos novos desafios que serão impostos pelo desenvolvimento tecnológico e pela cultura de proteção de dados pelos cidadãos.

2.2 DO TRATAMENTO DE DADOS PESSOAIS À LUZ DA LGPD

O objetivo central do presente trabalho foi analisar se o tratamento de dados pessoais realizado pelo Poder Judiciário está de acordo com as normas da Lei Geral de Proteção de Dados. Assim, se faz necessário abordar, neste primeiro capítulo, os conceitos básicos de tratamento de dados pessoais previstos na lei, os princípios previstos no art. 6º e as bases legais dos arts. 7º e 11º que o norteiam. Para isso, se faz necessário iniciar com o conceito de dado pessoal.

2.2.1 Do conceito de Dado Pessoal

O dado pessoal é um dos elementos mais importantes regulados pela LGPD e o componente central de diversas atividades econômicas e públicas. É possível afirmar que o dado e informação não são sinônimos. O dado é o fato bruto, enquanto a informação será um produto de uma transformação do dado. O contexto que a informação está inserida, a finalidade, com fins de utilidade, e a associação de outras informações é que agregam valor à informação[31]. E pelo fato de a informação pessoal estar atrelada à

[29] BATAGLIA, Murilo Borsio; LEMOS, Amanda Nunes Lopes Espineira; FARRANHA, Ana Claudia. *Proteção de Dados Pessoais e Acesso à Informação*: Interfaces do Papel da Sociedade Civil no Processo Legislativo Brasileiro. In: XIX Encontro da ANPAD – EnANANPAD 2020. 14 a 16 de outubro de 2020. Disponível em: http://www.anpad.org.br/abrir_pdf.php?e=Mjg5NDA=. Acesso em: 27 nov. 2021.
[30] DATA PRIVACY BRASIL. *Privacidade e proteção de dados no Congresso Nacional*. Disponível em: https://www.observatorioprivacidade.com.br/projetos-em-numeros/. Acesso em: 21 ago. 2021.
[31] RODOTÁ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 77.

proteção da personalidade[32], ela foi destacada para regulação do seu tratamento pela LGPD.

A LGPD traz destaque para três tipos de dado: o dado pessoal, dado sensível e dado anonimizado. O conceito de Dado Pessoal pela LGPD está previsto no artigo 5º, I, que diz que é toda "informação relacionada a pessoa natural identificada ou identificável". O dado pessoal sensível é definido no artigo 5º, II, como: "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, vinculado a uma pessoa natural". Por fim, já o dado anonimizado é definido no artigo 5º, III, como: "dado relativo à titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento".

Destaca-se que a definição de dado pessoal pode ter uma orientação mais reducionista ou expansionista[33]. Para Bruno Bioni "o vocabulário para prescrever tal definição é composto por palavras que restringem ou alargam o gargalo dessa proteção. Há uma bipartição do seu léxico que ora retrai (reducionista), ora expande (expansionista), a moldura normativa de uma lei de proteção de dados pessoais"[34]. Em paralelo com o conceito de dado pessoal, temos o uso das palavras "identificada" e "identificável". É possível definir o primeiro termo como reducionista, por tratar-se de apenas uma determinada ou específica pessoa. Já o segundo termo abrangeria uma pessoa que não é determinada e amplia seu espectro de alcance.

Dito isso, é possível dizer que a LGPD abarcou a orientação expansionista, por contemplar o termo "identificável" em sua redação. Isso torna-se relevante, uma vez que a depender do tipo de informação que se encontra no banco de dados e da análise

---

[32] CATALA, Pierre. "Ebauche d'une théorie juridique de l'information". 2021, p. 20. *In*: DONEDA, Danilo. *Da privacidade à proteção de dados*: elementos da formação da lei geral de proteção de dados. E-book. 2021.

[33] A temática do expansionismo e reducionismo em relação ao dado pessoal é descrita por Paul M. Schwartz e Daniel J. Solove no artigo "The PII Problem: Privacy and a New Concept of Personally Identifiable Information". Disponível em: https://ssrn.com/abstract=1909366. Acesso em 23 ago. 2021.

[34] BIONI, Bruno Ricardo. *Proteção de Dados Pessoais*: a função e os limites do consentimento. 3. Ed. Rio de Janeiro: Forense, 2021. p. 59.

contextual[35], [36], o dado pode ou não ser considerado pessoal[37]. Para que uma pessoa seja "identificável", conforme ensina Sombra, deve-se considerar que os meios e tecnologias disponíveis sejam capazes de, concretamente, fazer essa identificação. É possível ocorrer em um momento posterior, caso o agente de tratamento tenha meios para processar esses dados pessoais.[38]

A LGPD possui um rol exemplificativo no art. 5º que define os dados pessoais e caracteriza-os com uma visão expansionista. Pelo dado pessoal ter sido definido como "informação relacionada a pessoa natural identificada ou identificável", é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo, um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular"[39]. Por outro lado, o dado será anonimizado se for referente a uma pessoa indeterminada e se não for possível identificá-la. Conforme entendimento de Laura Mendes, o dado anônimo, em um primeiro momento, não estaria submetido pelo regramento da proteção de dados pessoais, visto que se por algum recurso tecnológico for possível a identificação da pessoa, este dado se tornará anonimizado[40].

O dado anonimizado, por conta da possibilidade de reversão de um processo de anonimização[41] e da sua falibilidade, deve sempre levar em consideração a análise contextual da base de dados, ou a conjugação de mais de uma. Ao considerar a adoção do

---

[35] Bioni, tanto no seu livro "Proteção de Dados Pessoais: a função e os limites do consentimento", como no trabalho "Xeque-mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil", traz alguns exemplos de como a análise contextual é influenciada nas estratégias reducionistas e expansionistas do conceito de dado pessoal.

[36] A perspectiva contextual da proteção de dados pessoais, além da perspectiva pluralista é reforçada por Thiago Sombra em sua obra "Fundamentos da regulação da privacidade e proteção de dados pessoais: pluralismo jurídico e transparência em perspectiva" (SOMBRA, 2019, p. 158).

[37] SOMBRA, Thiago Luís Santos. *Fundamentos da regulação da privacidade e proteção de dados pessoais*: pluralismo jurídico e transparência em perspectiva. 2019. p. 61.

[38] SOMBRA, Thiago Luís Santos. *Fundamentos da regulação da privacidade e proteção de dados pessoais*: pluralismo jurídico e transparência em perspectiva. Op. cit. p. 159.

[39] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679. Acesso em: 23 ago. 2021.

[40] MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. Editora Saraiva Jur, 2017. p. 57-58.

[41] Na União Europeia, antes do RGPD, os debates sobre a temática da proteção de dados e privacidade eram realizados por meio do Grupo de Trabalho do art. 29 (da Diretiva 95/46/EC). Desses encontros eram elaborados documentos, para fins de orientação. No caso de dados anonimizados, cabe mencionar a "*Opinion 05/2014 on Anonymisation Techniques*". Disponível em: https://ec.europa.eu/justice/article29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Acesso em: 23 ago. 2021.

conceito expansionista de dados pessoais pela LGPD, um critério de razoabilidade (nos artigos 5º, XI e 12º, § 1º da LGPD[42]) foi adotado, para que haja uma delimitação de até que ponto é possível correlacionar o dado a uma pessoa identificável. A razoabilidade, por ser um conceito indeterminado, foi utilizada pelo legislador para não eleger apenas uma técnica, e sim, por meio de outras técnicas desenvolvidas com a evolução tecnológica e que poderão ser alteradas posteriormente pelo legislador.

Ainda assim, é importante mencionar que os dados anonimizados que forem usados para formação de perfil comportamental serão considerados pessoais, pois o impacto desse tratamento afeta diretamente o titular dos dados, conforme artigo 12, § 2º da LGPD: "poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada", bem como nos casos de decisões automatizadas, previsto no artigo 20 da LGPD[43], que atinja os interesses do titular dos dados por meio de diversos perfis[44].

Por fim, diante dos conceitos trazidos, é possível observar a importância da regulação do dado pessoal e de suas especificações, uma vez que ele se relacionará com as questões sociais e econômicas que impactarão o cotidiano de seu titular. A visão expansionista do conceito de dado pessoal trazida pela LGPD, dá o direito do titular de exercer a autodeterminação informacional dos dados, ou seja, exercer o controle da proteção dos seus dados, o que será melhor abordado nos capítulos a seguir. Portanto, os dados pessoais representam projeções da pessoa humana e fazem parte dos direitos da personalidade. Sua proteção ganhou notoriedade e importância ao longo dos anos. Para a Lei Geral de Proteção de Dados, todo dado pessoal tem importância e valor. Por essa razão se adotou conceito amplo de dado pessoal, assim como estabelecido no Regulamento europeu (GDPR - *General Data Protection Regulation*), e definido como informação relacionada a pessoa natural identificada ou identificável. Por mais que alguns dados pareçam irrelevantes ou que não se referem a alguém diretamente, quando

---

[42] Art. 5º, XI: anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. (...) Art. 12, § 1º: A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

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

[44] BIONI, Bruno Ricardo. *Proteção de Dados Pessoais*: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021. p. 75-79.

transferidos, cruzados ou organizados, podem resultar em dados bastante específicos sobre determinada pessoa e trazer informações de caráter sensível, motivo que sua proteção deve ser realizada com mais atenção e efetividade.

2.2.2 Das Bases Legais previstas nos arts. 7º e 11º, da LGPD

O art. 1º da LGPD prevê que qualquer pessoa que trate dados, seja ela natural ou jurídica, de direito público ou privado, na atividade realizada nos meios digitais ou não, deverá ter uma base legal para fundamentar os tratamentos de dados pessoais que realizar. Isso importa dizer que não sendo uma hipótese de exclusão prevista no art. 4º, da LGPD, deverá ocorrer o tratamento em pelo menos uma das hipóteses legais para ser considerado legítimo e lícito. Não existe hierarquia entre elas, uma vez que a escolha da hipótese legal pelo agente de tratamento de dados se dará conforme a finalidade da atividade de tratamento a ser realizada, de modo que todas as opções previstas pelo legislador poderão ser utilizadas a partir de cada caso concreto, sem que uma tenha peso maior sobre a outra.

A partir dessas considerações iniciais, passar-se-á à análise do que é considerado tratamento regular e irregular de dados, para, posteriormente, adentrar-se especificamente nas hipóteses legais, constantes do art. 7º e 11º da LGPD. Para haver regularidade no tratamento de dados pessoais em uma situação fática, esta deverá ser aplicada a uma das hipóteses legais previstas no art. 7º da LGPD, ou, no caso de tratamento de dados sensíveis, em uma das hipóteses previstas no art. 11 da LGPD, sendo que o rol de cada um dos referidos dispositivos legais é taxativo,[45]logo, a Lei Geral de Proteção de Dados, ao mesmo tempo que é taxativo e limitador, permite o tratamento de dados pessoais com vistas a distinguir o tratamento regular do tratamento irregular de dados.

Contudo, é importante esclarecer que para o tratamento ser considerado regular não basta fundamentá-lo em uma das hipóteses legais previstas na lei, pois também é preciso que seja observada a boa-fé do operado e do controlador, bem como deverão ser respeitados os princípios norteadores previstos no art. 6º da LGPD (finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização).

---

[45] Os citados autores esclarecem o seguinte sobre o rol do art. 7º e do art. 11 da LGPD: "Entende-se que tanto o rol do Art. 7.º quanto o do Art. 11 são taxativos, sendo dotados de algumas hipóteses mais abertas e com certo grau de subjetividade (como, por exemplo, o legítimo interesse)" (BIONI, Bruno; DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otávio Luiz. *Tratado de Proteção de Dados Pessoais*. Editora Forense, 2021. p. 119).

Por outro lado, apresenta-se como irregular o tratamento de dados que é feito com a inobservância às hipóteses previstas na lei, ou ainda quando não fornecer a devida segurança que o titular de dados dele espera, consideradas situações como: a forma como o tratamento é realizado, o resultado, bem como os perigos ansiados, além das técnicas de tratamento de dados disponíveis no momento em que foi realizado.[46]

Caso seja constatado o uso irregular dos dados pessoais, na ocorrência de danos, estabelece o art. 42, §1º, inciso I da LGPD, que a responsabilidade do operador será solidária pelos danos causados pelo tratamento de dados, caso não obedeça às obrigações estabelecidas na lei ou se não tiver observado as instruções lícitas do controlador. Além disso, conforme estabelecido no inciso II do referido artigo, no caso de dano, o controlador diretamente envolvido no tratamento também será responsável de forma solidária.[47] Assim, cabe ao titular de dados optar por ajuizar a ação em face do controlador e/ou do operador.

Na linha dessa atenção dada às situações de tratamentos irregulares que podem ocorrer, cumpre enaltecer o microssistema jurídico inaugurado pela LGPD, o qual traz instrumentos que colocam o titular de dados no controle sobre suas informações pessoais (a denominada autodeterminação informativa que foi elegida como um dos fundamentos da LGPD, em seu art. 2º, inciso II e consiste no poder de escolha de quais dados serão utilizados, bem como os limites e a duração desse manuseio).

Portanto, respeitados os critérios autorizativos do tratamento de dados, como a utilização dos dados pessoais para finalidades legítimas e determinadas, respeito ao dever de informação ao titular sobre a realização do tratamento com suas informações, e, como dito, previsão do tratamento de dados, em algum dos referidos dispositivos (art. 7º e art. 11, ambos da LGPD), não há o que temer. Assim, inexistirá insegurança ou dificilmente

---

[46] NUNES, Natália Martins. *O tratamento irregular de dados pessoais e o dever de reparar os danos causados*. 2018. Disponível em: https://ndmadvogados.com.br/artigos/o-tratamento-irregular-de-dados-pessoais-e-o-dever-de-reparar-os-danos-causados. Acesso em: 21 set. 2021.

[47] "Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. § 1º A fim de assegurar a efetiva indenização ao titular dos dados: I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei; II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei" (BRASIL. *Lei n. 13.709, de 14 de agosto de 2018*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 21 set. 2021).

ocorrerão problemas quando o tratamento de dados realizado estiver consubstanciado na lei.

Desse modo, todos aqueles submetidos a essa norma necessitam entender e facilmente visualizar em quais situações, bem como atendidos quais pressupostos, será possível realizar tratamento de dados, de forma a não incidirem nas sanções civis e administrativas previstas na lei. O art. 7º da LGPD prevê as seguintes bases legais para o tratamento de dados (não sensíveis): consentimento (I); cumprimento de obrigação legal ou regulatória pelo controlador (II); execução de políticas públicas pela administração pública (III); realização de estudos por órgão de pesquisa (IV); execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido dele (V); exercício regular de direitos em processo judicial, administrativo ou arbitral (VI); proteção da vida ou da incolumidade física do titular ou de terceiros (VII); tutela da saúde, exclusivamente em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária (VIII); legítimo interesse (IX) e proteção do crédito (X). Destaca-se que nem todas as bases legais serão vistas de forma detalhada, por não serem o foco central do presente trabalho. Serão analisadas as bases legais dos incisos I, II, III, VI e IX, do art. 7º da lei, que são as bases legais mais utilizadas pelo Poder Público.

2.2.2.1 *Consentimento Informado*

O art. 7º, I, LGPD prevê a base legal do consentimento. Já o art. 5º, XII, LGPD conceitua o consentimento como a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". Já no caso de dados sensíveis, o consentimento deve ser fornecido "de forma específica e destacada, para finalidades específicas" (art. 11, I, LGPD). Assim, é importante o titular do dado saber de forma clara para qual finalidade seus dados serão tratados e sua autorização deve ser intencional, sendo vedada a autorização tácita e para finalidades genéricas.

O §1º do art. 9º, LGPD prevê que caso as informações solicitadas ao titular forem de conteúdo enganoso ou abusivo, apresentadas sem prévia transparência, sem clareza e de forma inequívoca, o consentimento será considerado nulo. Já o *caput* do art. 8º da lei, estabelece que o consentimento deve ser apresentado por escrito ou por outro meio que demonstre a manifestação de vontade do titular de dados. Ainda assim, é importante

mencionar que da mesma forma que o titular é livre para manifestar seu consentimento, ele também é para revogá-lo a qualquer momento, de forma expressa e inequívoca[48], conforme prevê o art. 8º, §5º da LGPD[49], pois o agente de tratamento pode alterar a finalidade do tratamento, tornando o consentimento do titular incompatível com os referidos objetivos iniciais. A fim de permitir facilidade ao titular para manifestar sua concordância e revogação, cabe ao controlador dispor de meios apropriados a essa finalidade, especialmente de cunho tecnológico, para realizar a devida gestão e controle relativos a essa base legal.

Tratando-se do Poder Público, o consentimento não será a base legal mais apropriada para o tratamento de dados pessoais, principalmente quando o tratamento for necessário para o cumprimento de obrigações e atribuições legais. Nesses casos, o órgão ou a entidade exerce prerrogativas estatais típicas, que se impõem sobre os titulares em uma relação de desbalanceamento de forças, na qual o cidadão não possui condições efetivas de se manifestar livremente sobre o uso de seus dados pessoais.

Portanto, a utilização dessa base legal no âmbito do tratamento de dados pessoais pelo Poder Público pressupõe assegurar ao titular a efetiva possibilidade de autorizar ou não o tratamento de seus dados, sem que sua manifestação de vontade resulte em restrições significativas à sua condição jurídica ou ao exercício de direitos fundamentais.

2.2.2.2 *Cumprimento de Obrigação Legal ou Regulatória pelo Controlador*

O inciso II, do art. 7º, da LGPD prevê a base legal de tratamento de dados pessoais por cumprimento de obrigação legal ou regulatória pelo controlador, ou seja, para que seja possível que o controlador legitime o tratamento de dados pessoais que realiza por meio dessa base legal, ele precisará justificar a utilização do dado pessoal para atender

[48] Sobre a revogabilidade do consentimento, Doneda correlaciona essa possibilidade conferida ao titular aos direitos da personalidade com a seguinte afirmação: "A ideia de sua revogabilidade incondicional encontra fundamento no fato de se estar protegendo a própria personalidade, entre cujos atributos estaria a indisponibilidade. Por esse ponto de vista, tal consentimento será sempre revogável e a sua caracterização como ato jurídico unilateral serve a reforçar essa revogabilidade" (DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2. ed. Rio de Janeiro: Revista dos Tribunais, 2019. p. 303).

[49] Doneda pontua também sobre a possibilidade de revogação do consentimento o seguinte: "Examinando a natureza do instituto e dos interesses em questão, deve-se reconhecer a possibilidade de revogação do ato pelo qual uma pessoa consente no tratamento de seus dados pessoais, visto que nesse seu poder encontra-se o próprio sentido de autodeterminação em relação à construção de sua esfera privada. Esse poder, ligado ao livre desenvolvimento da personalidade, merece, portanto, a tutela do ordenamento jurídico" (DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2. ed. Rio de Janeiro: Revista dos Tribunais, 2019. p. 304).

uma obrigação legal ou regulatória. A mesma hipótese está prevista no art. 11, II, a que rege o tratamento de dados sensíveis. De forma geral, a aplicação desses dispositivos será efetuada em dois contextos normativos distintos, que se diferenciam em razão da espécie de norma jurídica que estabelece a obrigação a ser cumprida. É o caso, em especial, das normas de conduta e das normas de organização[50].

Na primeira hipótese, a obrigação legal decorre de uma norma de conduta, isto é, uma regra que disciplina um comportamento, em geral estabelecendo um fato ou uma hipótese legal, com uma possível consequência jurídica em caso de descumprimento. Caso o responsável não cumpra a obrigação legal (como, por exemplo, a divulgação da agenda de compromissos públicos de autoridades, conforme art. 11 da Lei nº. 12.813/2013), poderá ser objeto das penalidades administrativas previstas na legislação[51].

Nessas situações, o tratamento de dados pessoais é necessário para atender a uma regra específica, ou seja, uma determinação legal expressa ou uma obrigação de natureza regulatória estabelecida por um órgão regulador. Não há, por isso, um vínculo necessário e direto entre o tratamento de dados e o exercício de atribuições e competências legais do controlador. Já na segunda hipótese, a obrigação legal decorre de normas de organização, assim entendidas as normas que estruturam órgãos e entidades e estabelecem suas competências e atribuições[52]. Nesse contexto normativo, o tratamento de dados pessoais é parte essencial do exercício de prerrogativas estatais típicas, uma vez que é necessário para viabilizar a própria execução das atribuições, competências e finalidades públicas da entidade ou do órgão público.

Assim, diferentemente das normas de conduta que estabelecem obrigações de forma direta e expressa, prevendo uma consequência específica em caso de

---

[50] Um terceiro tipo de obrigação pode decorrer de "normas-objetivo" ou "normas programáticas", que estabelecem objetivos e metas a serem alcançados por entidades e órgãos públicos. Nestes casos, porém, a ação estatal costuma ser materializada por meio da definição e execução de políticas públicas, base legal específica, objeto de comentário na próxima seção.

[51] As normas de conduta "são aquelas destinadas a reger, diretamente, as relações sociais e o comportamento das pessoas. Normas de conduta [...] preveem um fato e a ele atribuem um efeito jurídico. São concebidas na forma de um juízo hipotético: se ocorrer *F*, então *E*. Por exemplo: em se verificando o fato gerador, será devido o tributo; se o contrato for violado, a parte responsável deverá pagar uma indenização" (BARROSO, L. R. *Curso de direito constitucional contemporâneo*. São Paulo: Saraiva, 2009, p. 192).

[52] Segundo Luís Roberto Barroso, as normas de organização "contêm uma prescrição objetiva, uma ordem para que alguma coisa seja feita de determinada maneira. Não contêm um juízo hipotético, mas um mandamento taxativo. Em lugar de disciplinarem condutas, as normas de organização, também chamadas de normas de *estrutura*, instituem órgãos, atribuem competências, definem procedimentos" (BARROSO, 2009, p. 193). Em sentido similar, para Miguel Reale, o que caracteriza uma norma de organização "é a *obrigação objetiva de algo que deve ser feito*, sem que o dever enunciado fique subordinado à ocorrência de um fato previsto, do qual possam ou não resultar determinadas consequências" (grifo conforme o original). *Lições preliminares de direito*. 25. ed. São Paulo: Saraiva, 2001, p. 87-88.

descumprimento, as normas de organização estabelecem obrigações que estão associadas, de forma mais geral, ao próprio cumprimento e à execução de atribuições legais típicas da entidade ou do órgão público responsável pelo tratamento de dados pessoais.

Tratando-se do Poder Público, a referida base é a mais utilizada como justificativa de tratamento de dados pessoais e essa interpretação do conceito de obrigação legal, conforme previsto no art. 7º, II, e no art. 11, II, *a*, da LGPD, é reforçada pelo disposto no art. 23 da mesma lei. Assim, o tratamento de dados pessoais no setor público deverá ser realizado "com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público", observando-se o interesse público e o atendimento da finalidade pública do controlador, o que será melhor visto a frente ao tratar do tratamento de dados pelo Poder Público.

2.2.2.3 *Execução de Políticas Públicas pela Administração Pública*

O inciso III, art. 7º, da LGPD, prevê a base legal de tratamento de dados pessoais pela Administração Pública que visa o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV da lei, que regula o tratamento de dados pessoais pelo Poder Público.

O conceito de "administração pública" deve ser delimitado a partir da definição de Poder Público. Abrange tanto órgãos e entidades do Poder Executivo quanto dos Poderes Legislativo e Judiciário, inclusive das Cortes de Contas e do Ministério Público, desde que estejam atuando no exercício de funções administrativas, com vistas à execução de políticas públicas. A execução de políticas públicas é uma das maiores justificativas para que o setor público realize tratamentos de dados. Assim, é recomendado que o conceito de política pública seja interpretado de forma ampla, de modo a abranger qualquer programa ou ação governamental, definido em instrumento formal, isto é, lei, regulamento ou ajuste contratual, conforme o caso, cujo conteúdo inclui, em regra, objetivos, metas, prazos e meios de execução.

Portanto, no que tange à execução de políticas públicas, é importante destacar o art. 23 da LGPD, que prevê a exigência de que o tratamento seja realizado para o atendimento da finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde

que: a) sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos; e b) seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais.

2.2.2.4 *Exercício regular de direitos em processo judicial, administrativo ou arbitral*

O tratamento também pode ter como base o exercício regular de direitos em processo judicial, administrativo ou arbitral (nos termos da Lei nº 9.307/96 – Lei da Arbitragem), conforme previsto no inciso VI, do art. 7º, da LGPD. Essa base legal é ampla, pois autoriza o uso de dados pessoais em processos para garantir o direito de produção de provas de uma parte contra a outra, o que garante o direito à ampla defesa e ao contraditório. Compreende como exercício regular de direitos, ações do cidadão comum autorizadas pela existência de direito definido em lei e condicionadas à regularidade do exercício desse direito. Dentro dessa hipótese, não pode haver conduta abusiva ou o desempenho disfuncional de certa posição jurídica pela parte. Portanto, para dados que poderão servir como elementos para o exercício de direitos em demandas, poderão ser armazenados, desde que havendo real necessidade e para essa finalidade.

2.2.2.5 *Legítimo Interesse e a vontade do titular de dados como limitador*

A base legal do legítimo interesse prevista no inciso IX, do art. 7º, da LGPD autoriza o tratamento de dados pessoais de natureza não sensível quando necessário ao atendimento de interesses legítimos do controlador ou de terceiros, “exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais”. Portanto, não é aplicável ao tratamento de dados pessoais sensíveis.

Sua aplicação deve visar a proporcionalidade entre, de um lado, os interesses do controlador ou de terceiros para a utilização do dado pessoal e, de outro, os direitos e as legítimas expectativas do titular, o que a caracteriza como uma base legal flexível. Ademais, deve levar em consideração o art. 18, § 2º, que prevê de o titular ter o direito de se opor ao tratamento realizado com base no legítimo interesse, em caso de descumprimento dos requisitos previstos na LGPD. Tratando-se do Poder Público, a

aplicação do legítimo interesse é limitada, o que se assemelha com o consentimento, uma vez que sua aplicação não é apropriada quando o tratamento de dados pessoais é realizado de forma compulsória ou quando houver necessidade de cumprimento de obrigações e atribuições legais do Poder Público.

Por isso, recomenda-se que os órgãos e entidades públicas evitem recorrer ao legítimo interesse, preferindo outras bases legais para justificar os tratamentos de dados pessoais, como a de execução de políticas públicas e cumprimento de obrigação legal, pois será difícil realizar uma ponderação entre as expectativas dos titulares e os supostos interesses estatais, visto que estes, por definição legal ou regulamentar, conforme o caso, tendem a estabelecer restrições aos direitos individuais nele envolvidos.

Desse modo, o legítimo interesse poderá eventualmente ser admitido como base legal para o tratamento de dados pessoais pelo Poder Público. Caso seja aplicado, a utilização dos dados não deve ser compulsória, e a atuação estatal não deve se basear no exercício de prerrogativas estatais típicas, que decorrem do cumprimento de obrigações e atribuições legais. Contudo, é necessário discorrer sobre a influência da vontade do titular de dados sobre essa base, a partir do pressuposto de que o direito à privacidade ou o direito à proteção de dados[53] é disponível.

A vontade do titular tem enorme relevância jurídica no exame das situações concretas, especialmente, quando houver dúvida a respeito da incidência de outras bases normativas ao caso. Assim, quando houver alguma oposição do titular ao tratamento de dados que se baseia na base do legítimo interesse, é importante analisar se há alguma consequência jurídica. Trata-se de cláusula geral essa hipótese legal, a qual, diante de sua abertura semântica, demanda maior esforço hermenêutico do intérprete e aplicador da lei. De fato, para a análise das situações nas quais essa hipótese incide, deve ser realizada detida atividade de ponderação, na qual a vontade do titular deve ser considerada, ainda que num segundo momento (*opt out*)[54].

Nesse sentido, o art. 10 da LGPD dispõe que o legítimo interesse do controlador apenas poderá justificar tratamento de dados a partir de situações concretas "que incluem,

---

[53] Enfatiza-se, novamente, conforme pontua Bessa, que a despeito de haver certa divergência conceitual, especialmente em relação à autonomia do direito à proteção de dados pessoais sobre o direito à privacidade, há concordância quanto ao fato de se tratarem de importantíssimas diretrizes hermenêuticas quando da aplicação da LGPD (BESSA, Leonardo Roscoe. *LGPD: direito ou dever de privacidade?* 2003. Disponível em: https://www.conjur.com.br/2021-fev-08/leonardo-bessa-lgpd-direito-ou-dever-privacidade. Acesso em: 02 nov. 2021).

[54] BIONI, Bruno. *Proteção de dados pessoais. A função e os limites do consentimento*. 3. ed. Rio de Janeiro: Forense: 2021. p. 248.

mas não se limitam a: I - apoio e promoção de atividades do controlador; e II - proteção em relação ao titular do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei"[55]. Verifica-se que esse dispositivo direciona sua compreensão à análise da situação concreta, além de trazer algumas hipóteses nas quais serão justificáveis o tratamento de dados com fundamento no legítimo interesse.

Logo, a autonomia da vontade e a autodeterminação informativa são balizas presentes na lei brasileira de proteção de dados, as quais visam assegurar o respeito aos direitos fundamentais dos titulares, assim, a vontade do titular, embora destacada na base legal do consentimento informado (art. 7º, inciso I e art. 11, inciso I da LGPD), também é relevante e necessária na ponderação feita pelo intérprete ao utilizar a base legal do legítimo interesse. Portanto, a vontade do titular, por mais que não se trate de um direito absoluto, por poder sofrer restrição pelo legislador, deverá ser considerada quando for aplicado a base legal do legítimo interesse para ponderações pelo intérprete, ainda que depois da ocorrência do tratamento.

2.3 TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS – ART 11º, LGPD

Após analisar as bases legais para o tratamento de dados pessoais, é necessário apresentar algumas informações relevantes sobre o tratamento dos dados pessoais sensíveis, aos quais são dados que merecem mais atenção e proteção, pois envolvem a privacidade, intimidade dos cidadãos e oferecem mais riscos discriminatórios aos titulares. Os dados pessoais chamados sensíveis se encontram presentes em todos os conjuntos informacionais do ser humano. Segundo o art. 5º, inciso II, da LGPD, dados sensíveis versam sobre origem racial ou étnica, convicção religiosa, opinião política e filiação a sindicato ou a organização de caráter religioso, filosófico ou político, à saúde ou à vida sexual e dados genéticos ou biométricos.

Trata-se de dados sensíveis do ponto de vista dos direitos e liberdades fundamentais, por propiciar riscos significativos para seu titular. Integram a privacidade e intimidade do titular, tendo em vista que, pelo tipo e natureza de informação que trazem, o tratamento pode ensejar a discriminação de seu titular, e por isso, devem ser protegidos

[55]BRASIL. *Lei n. 13.709, de 14 de agosto de 2018*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 02 nov. 2020.

de forma mais rígida[56]. As bases legais previstas no art. 11 da LGPD são destinadas às situações de tratamento de dados pessoais sensíveis, os quais, em razão de representarem maior potencial de danos aos titulares, devem ser usados com a máxima cautela possível.[57] Ao comparar as hipóteses legais previstas no art. 7º com as do art. 11, da LGPD, percebe-se que no tratamento de dados sensíveis foram suprimidas as seguintes bases previstas naquele artigo: (v) execução de contrato; (x) proteção do crédito; e (ix) legítimo interesse, sendo que as demais poderão ser aplicadas aos dados sensíveis.

Assim, ao utilizar uma base legal para o tratamento de dados sensíveis é necessário verificar a potencialidade discriminatória e lesiva que certos dados pessoais, ao serem tratados, podem ocasionar aos seus titulares, especialmente quando se estiver diante de dados aos quais, em um primeiro momento, não sejam considerados passíveis de gerar danos ao titular, mas que, a partir de sua junção com outras informações, possam vir a gerar[58].

Com efeito, um dos princípios norteadores previstos no art. 6º, inciso IX da LGPD é o da não discriminação, que consiste na "impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos". Percebe-se, portanto, que a finalidade da lei na proteção dos dados sensíveis é assegurar uma igualdade substancial no tratamento de dados, proibindo, dessa forma, qualquer tipo de discriminação e abuso que dele possa decorrer.[59]

Portanto, os dados sensíveis necessitam de uma tutela diferenciada e especial, de forma a se evitar que informações dessa natureza sejam vazadas, usadas indevidamente, comercializadas ou sirvam para embasar preconceitos e discriminações ilícitas em relação

---

[56] RODOTÁ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 78 e 96.

[57] Viola e Teffé salientam que se tratam de dados "(...) especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, cujo conteúdo propicia riscos significativos para seu titular. Eles integram o "núcleo duro" da privacidade, tendo em vista que, pelo tipo e natureza de informação que trazem, apresentam informações cujo tratamento pode ensejar a discriminação de seu titular, devendo, por conseguinte, ser protegidos de forma mais rígida" (BIONI, Bruno; DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otávio Luiz Rodrigues. *Tratado de Proteção de Dados Pessoais*. Editora Forense, 2021. p. 139).

[58] Assim: "não só a natureza de um dado estruturalmente considerado deve ser avaliada para sua determinação como sensível, mas deve-se admitir que certos dados, ainda que não tenham, a princípio, essa natureza especial, venham a ser considerados como tal, a depender do uso que deles é feito no tratamento de dados. Por exemplo, se considerarmos numa base de dados o nome e o bairro em que uma pessoa mora, pode ser possível identificar a origem racial desta pessoa. Significa dizer que no tratamento de dados pessoais, em que se consideram estes dois dados não sensíveis, pode-se chegar à determinação de um dado sensível – raça – que, por sua vez, pode gerar consequências no tratamento de dados indesejadas, discriminatórias ou prejudiciais a seu titular" (MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais. *Revista do Advogado*, n. 144, p. 49, nov. 2019).

[59] MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais. *Revista do Advogado*, n. 144, p. 50, nov. 2019.

ao titular. Todavia, a mera proibição do tratamento de dados sensíveis é inviável, pois, em alguns momentos, o uso de tais dados será legítimo e necessário, além do que existem determinados organismos cuja própria razão de ser estaria comprometida caso não pudessem obter informações desse gênero, como, por exemplo, algumas entidades de caráter político, religioso, filosófico e processual. Esse último será melhor analisado no capítulo 2 deste trabalho ao ser abordada a exposição desses dados no processo judicial eletrônico, com acesso livre de terceiros que não possuem vínculo direto ao processo judicial, e como melhor protegê-los.

2.4 TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

Após análise dos conceitos e regras gerais trazidos pela LGPD ao tratamento de dados pessoais, se faz necessário o aprofundamento do tema no âmbito do Poder Público, que é o foco do presente trabalho por tratar-se especificamente do Poder Judiciário, que faz parte da Administração Pública. O legislador dedicou o Capítulo IV da LGPD para estabelecer as regras às quais o Poder Público deve se submeter ao realizar o tratamento de dados pessoais dos cidadãos. Ao considerar que um dos objetivos da Lei é a proteção do titular de dados contra intromissões em sua vida privada e o uso arbitrário de suas informações pessoais, é essencial o Estado e demais órgãos do poder público seguirem as regras previstas na LGPD de proteção de dados pessoais, de modo a evitar o comprometimento dos direitos de personalidade.

O artigo 23 da LGPD prevê que o tratamento de dados pessoais pelas pessoas jurídicas de direito público previstas na Lei nº. 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) deve sempre ser realizado para o "atendimento de uma finalidade pública, na persecução do interesse público e com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público", e define que as informações sobre o tratamento realizado devem ser claras e expostas em veículos de fácil acesso, dando preferência a sítios eletrônicos. Logo, o caput do artigo estabelece dois princípios da Administração Pública que vinculam o tratamento de dados pelo Poder Público: a finalidade pública e a supremacia do interesse público.

O princípio da finalidade está contido no princípio da legalidade e dispõe que as atividades da Administração Pública deverão ser focadas e limitadas aos dispositivos normativos autorizadores de tais atividades, ou seja, esse princípio limita o poder da Administração Pública ao exigir que atue dentro dos limites de suas normas, de modo a

impedir atos abusivos contra os cidadãos[60]. O princípio da supremacia do interesse público, por sua vez, tem como objetivo preservar e realizar o interesse de toda a sociedade. É dizer que o interesse público se sobrepõe aos interesses privados.

Conforme prescreve Barroso[61], o debate contemporâneo divide o interesse público em primário e secundário. O interesse público primário se consubstancia nos fins a que cabe promover no interesse de toda a sociedade, quais sejam a justiça, a segurança e o bem-estar social. Já o interesse público secundário se refere ao interesse da pessoa jurídica de direito público que é parte em determinada relação jurídica e pode ser traduzido como o interesse do erário, composto pela maximização da arrecadação e pela minimização das despesas. É dessa distinção que decorrem as esferas constitucionais de atuação do Ministério Público, a quem cabe defender o interesse público primário, e da Advocacia Pública, a quem cabe a defesa do interesse público secundário[62].

Desta feita, em que pese a LGPD prever em seu art. 6º os princípios que devem reger o tratamento de dados de forma geral, o Poder Público está vinculado a observar, precipuamente, os princípios da finalidade e interesse público, de modo que a atuação do Poder Público é excepcional e condicionada. Vale destacar que a aplicação do artigo em análise, depreende-se também ao Poder Judiciário, uma vez que se subordinam ao regime da Lei de Acesso à Informação[63] todas as pessoas jurídicas de direito público, inclusive os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo e Judiciário, bem como do Ministério Público.

Ainda, o art. 23 prevê expressamente que o tratamento de dados pessoais pelo Poder Público deverá ter como objetivo a execução de suas competências legais ou o cumprimento das atribuições legais do serviço público, o que significa que o Poder Público deve cumprir sua função legal de administrar a vida em sociedade e somente o

---

[60] AGRA, Walber de Moura. *Curso de direito constitucional*. p. 437.
[61] BARROSO, Luís Roberto. *Curso de Direito Constitucional Contemporâneo*: os conceitos fundamentais e a construção do novo modelo. p. 90.
[62] BARROSO, Luís Roberto. *Curso de Direito Constitucional Contemporâneo*: os conceitos fundamentais e a construção do novo modelo. p. 90.
[63] Art. 1º. Esta Lei dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do parágrafo 3º, do art. 37 e no parágrafo 2º, do art. 216 da Constituição Federal, Parágrafo único. Subordinam-se ao regime desta Lei:
I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público;
II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

pode fazer em observância e na medida em que a lei lhe dá investidura[64]. Já o art. 25, por sua vez, estabelece que os dados deverão ser mantidos sempre de forma estruturada e interoperável para uso compartilhado com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

Ao tratar do compartilhamento de dados pessoais, o artigo 26 deixa expresso que o uso compartilhado de dados pessoais pelo Poder Público deve atender os princípios de proteção de dados pessoais elencados no artigo 6º da LGPD que servem como filtros de validade e legitimidade das regras de proteção de dados pessoais, que se materializam ao se verificar que a execução das políticas públicas e o exercício das competências legais estão em equilíbrio com as liberdades positivas, caracterizadas pelo controle da atividade pública, e negativas, que se consubstanciam na preservação dos direitos e garantias fundamentais do titular de dados[65].

Para Tasso[66], os princípios da finalidade, da adequação e da responsabilização e prestação de contas, previstos, respectivamente, nos incisos I, II e X do art. 6º da LGPD, buscam fundamento de validade nos princípios constitucionais da legalidade, da impessoalidade e da moralidade e se materializam quando, cumulativamente, o ato administrativo de tratamento ou compartilhamento de dados pessoais: (i) está previsto em leis e regulamentos ou respaldado em contratos, convênios ou instrumentos congêneres, conforme prevê o art. 7º, III, da LGPD; (ii) é praticado no exercício de suas competências ou atribuições, nos termos do art. 23, da LGPD; e (iii) o ato praticado busca o atendimento do interesse público, conforme prevê o art. 23 da LGPD.

Já os princípios de transparência e do livre acesso, previstos nos incisos VI e IV do art. 6º da LGPD, respectivamente, possuem direta relação com o princípio da publicidade e são observados quando o órgão público: (i) pratica a transparência ativa, combinados o art. 23, I, da LGPD com o art. 8º da LAI; (ii) viabiliza a transparência passiva, combinados o art. 23, I da LGPD com o artigo 10 da LAI; (iii) implementa outras formas de publicidade das operações de tratamento preconizadas pela ANPD, previstas no art. 23, parágrafo 1º, da LGPD; e (iv) expede os informes e comunicados previstos no

---

[64] TASSO, Fernando Antonio; MALDONADO, Viviane N. Brega; BLUM, Renato Opice. *LGPD: Lei Geral de Proteção de Dados*. Coordenadores: MALDONADO, Viviane N brega; BLUM, Renato Opice. São Paulo: Revista dos Tribunais, 2019. p. 252.

[65] TASSO, Fernando Antonio. *In*: MALDONADO, Viviane N. Brega; BLUM, Renato Opice. *LGPD: Lei Geral de Proteção de Dados*. p. 274.

[66] TASSO, Fernando Antonio. *In*: MALDONADO, Viviane N. Brega; BLUM, Renato Opice. *LGPD: Lei Geral de Proteção de Dados*. p. 274.

art. 26, parágrafo 2º, e art. 27, II, da LGPD. Os princípios da necessidade ou da mínima coleta, qualidade dos dados e da segurança, dispostos, respectivamente, nos incisos III, V e VII do art. 6º da LGPD, possuem fundamento no princípio constitucional da eficiência, que juntamente com o princípio da não discriminação, previsto no inciso XI do referido artigo, fundamentado no princípio da legalidade e da boa-fé, fecham o escopo principiológico da LGPD.

Superados os princípios, verifica-se que o parágrafo 1º, do artigo 26, enumera, exaustivamente, as hipóteses autorizadoras da transferência de dados para entidades privadas, e é vedada a transferência não fundamentada na forma estabelecida na lei. Logo, cabe ao Poder Público garantir que o uso compartilhado de dados siga os propósitos especiais que concernem a execução das políticas públicas, e que, ao mesmo tempo, a ponderação entre a necessidade de publicidade das informações disponíveis ao acesso garante que os direitos dos titulares sejam respeitados[67].

O art. 27 da LGPD dispõe que a comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público à pessoa de direito privado deverá ser informada à autoridade nacional e dependerá de consentimento do titular, salvo se dispensado nos termos da lei, nos casos em que a publicidade já é decorrente do tratamento realizado no exercício das competências legais do Poder Público, e nas exceções do parágrafo 1º, do art. 26. Ainda assim, destaca-se que os órgãos públicos estão sujeitos a medidas administrativas específicas, ou seja, cabe à Autoridade Nacional de Proteção de Dados Pessoais (ANPD) garantir que medidas cabíveis e proporcionais sejam adotadas ao violarem o tratamento de dados pessoais nos órgãos públicos.

Por fim, diante desse cenário, o desafio posto pela LGPD é o de estabelecer parâmetros objetivos, capazes de conferir segurança jurídica às operações com dados pessoais realizadas por órgãos e entidades públicas, e assegurar a celeridade e a eficiência necessárias à execução de políticas e à prestação de serviços públicos com respeito aos direitos à proteção de dados pessoais e à privacidade. Como pessoa jurídica de direito público, autorizada por hipóteses legais a tratar dados, independentemente do consentimento do titular, o Poder Judiciário, através de seus órgãos jurisdicionais, é o controlador dos dados, a quem cabe o poder de decisão sobre o tratamento dos dados coletados em sua função administrativa ou jurisdicional, e, portanto, deve seguir todas as

[67] PINHEIRO, Patricia Peck. *Proteção de dados pessoais: comentários à Lei 13.709/2018 (LGPD).* São Paulo: Saraiva, 2018.

regras apresentadas de tratamento de dados, o que será melhor abordado no capítulo seguinte.

3 OS DESAFIOS ENFRENTADOS PELO PODER JUDICIÁRIO NA ADEQUAÇÃO ÀS NORMAS DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

No capítulo anterior foi feita uma análise histórica da evolução da proteção de dados no ordenamento jurídico brasileiro até a chegada da Lei Geral de Proteção de Dados Pessoais. Após, foram apresentados conceitos e regras trazidas pela lei sobre o tratamento de dados pessoais no âmbito privado e público, as quais serão de grande importância para o presente capítulo, uma vez que será analisado o tratamento de dados pessoais realizado pelo Poder Judiciário.

Desse modo, no presente capítulo, serão apresentados os desafios enfrentados pelo Poder Judiciário na adequação às normas da LGPD, como o da colisão dos direitos fundamentais da publicidade dos atos processuais, privacidade, intimidade e proteção de dados pessoais; se o Poder Judiciário possui legitimidade para aplicar as normas previstas na LGPD; se os dados coletados e armazenados pelos seus órgãos são passíveis de regulação e estão bem protegidos conforme as normas da lei; a exposição de dados pessoais em processos judiciais eletrônicos, decisões judiciais, jurisprudência; ataques frequentes de *Hackers* aos sistemas dos órgãos do judiciário; e compartilhamento de dados pessoais.

Contudo, antes de adentrar nesses desafios onde será discutido o sério problema enfrentado pelo Poder Judiciário de colisão de princípios fundamentais, se faz necessário apresentar os novos conceitos e alcance dos princípios que norteiam a proteção de dados, como o da privacidade e intimidade e que contribuíram para a evolução da proteção de dados pessoais para um direito fundamental e autônomo.

3.1 PARA ALÉM DO DIREITO À PRIVACIDADE E INTIMIDADE: A PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL E AUTÔNOMO

É importante apresentar a construção normativa da tutela jurídica da proteção de dados pessoais, desde sua concepção até a estruturação do microssistema legal brasileiro de proteção de dados pessoais, consolidado com a vigência da LGPD e como um direito fundamental autônomo. Porém, antes, será abordada a evolução histórica do direito fundamental à privacidade para compreender essa evolução da proteção de dados pessoais.

O surgimento do direito à privacidade no ordenamento jurídico deu-se através de decisões judiciais relacionadas às elites burguesas ao longo do século XX. Com a intensificação da vigilância e o controle das informações pessoais que visam garantir a eficiência e a redução dos custos com a produção, a classe operária passou a reconhecer a necessidade de invocar tal direito[68]. Por ser um direito com dimensão estritamente negativa e individualista, passou a ser considerado como pressuposto para o reconhecimento de outros direitos fundamentais[69] e apenas se popularizou a partir da década de 1960 com o advento do *Welfare State* e da conquista de direitos pelos movimentos sociais de massas.

Um dos momentos históricos marcantes em que a privacidade ganhou projeção em âmbito internacional foi após a Segunda Guerra Mundial, com o advento da Declaração Universal dos Direitos do Homem de 1948, que prevê, em seu art. XII, além do direito à privacidade, também o direito à honra e ao sigilo de correspondência[70]. Louis Brandeis e Samuel Warren foram marcantes, ao final do século XIX, que iniciaram a construção do conceito jurídico de privacidade, através do artigo *The Rigth to Privacy*[71]. A difusão da fotografia, dos jornais impressos, bem como revistas e atrações televisivas tomavam conta de assuntos que antes estavam reclusos à vida privada e aos ambientes domésticos americanos. Por isso, entendem que as novas técnicas e instrumentos tecnológicos passaram a possibilitar o acesso e a divulgação de fatos relativos à esfera privada do indivíduo como nunca antes.

Os conceitos iniciais de privacidade perpassavam a ideia de individualismo e trata o direito à privacidade como "o direito de ser deixado só". Essa visão trazia a noção de que "a privacidade seria um aspecto fundamental da realização da pessoa e do desenvolvimento da sua personalidade"[72], o que fez os autores associarem a privacidade

---

[68] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. São Paulo: Thomson Reuters, 2019, p. 33.
[69] MENDES, Laura Schertel. *Transparência e privacidade*: violação e proteção da informação pessoal na sociedade de consumo. 2008. 17 f. Dissertação (Mestrado em Direito) - Universidade de Brasília, Brasília, 2008.
[70] MENDES, Laura Schertel. *Transparência e privacidade*: violação e proteção da informação pessoal na sociedade de consumo. 2008. 17 f. Dissertação (Mestrado em Direito) - Universidade de Brasília, Brasília, 2008. p. 17.
[71] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. São Paulo: Thomson Reuters, 2019. p. 30.
[72] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. São Paulo: Thomson Reuters, 2019. p. 30.

ao direito de inviolabilidade da personalidade, pois até então a violação a proteção da vida privada era associada à propriedade[73].

Com o avanço dessas projeções, o direito à privacidade ganhou destaque com as novas transformações sociais ocasionadas pela revolução da tecnologia da informação e adquiriu reconhecimento no âmbito internacional, de modo que os ordenamentos jurídicos passaram não somente a se preocupar com a reparação dos danos causados pela violação desse direito, mas também a pensar em medidas de proteção[74]. Por outro lado, ao se tratar do direito à intimidade, há de registrar que em sua acepção clássica o direito à intimidade possui como âmbito de proteção material os aspectos mais interiores ou próximos do indivíduo, os quais formam o que se denomina zona íntima e reservada. Os pensamentos, ideias, emoções, o âmbito da vida pessoal e familiar diante da intromissão ilegal, correspondem ao direito fundamental à intimidade, o direito mais interior das pessoas, que é variável segundo o momento histórico. Busca-se, portanto, a tutela do segredo domiciliar, o profissional e das comunicações telefônicas.

Desse modo, o direito à intimidade é a forma mais restrita em relação à privacidade, o direito que a pessoa humana possui de distanciar indivíduos estranhos de informações ou fatos pessoais que não deseje compartilhar. Logo, visa proteger a parte da vida que a pessoa leva quando está distante da observação alheia. Assim, o direito à privacidade é mais amplo que o simples direito à intimidade, tendo em vista que o direito à privacidade abrange a intimidade e o sigilo. Assim sendo, a distinção entre o direito à privacidade e o direito à intimidade é uma questão de abrangência e não uma questão conceitual.

Para Leonardo Roscoe Bessa, "nem sempre há uma nítida distinção entre *o direito à vida privada e o direito à intimidade*. Há quem sustente que se trata de diferentes denominações do mesmo direito. O correto, entretanto, é o entendimento de que o segundo é espécie do primeiro, ainda que tal afirmação não traga, em princípio, consequências jurídicas diversas"[75].

---

[73] MENDES, Laura Schertel. *Transparência e privacidade*: violação e proteção da informação pessoal na sociedade de consumo. 2008. 15 f. Dissertação (Mestrado em Direito) - Universidade de Brasília, Brasília, 2008.

[74] MENDES, Laura Schertel. *Transparência e privacidade*: violação e proteção da informação pessoal na sociedade de consumo. 2008. 15 f. Dissertação (Mestrado em Direito) - Universidade de Brasília, Brasília, 2008. p. 18.

[75] BESSA, Leonardo Roscoe. *O consumidor e os limites dos bancos de dados de proteção ao crédito.* São Paulo: Editora Revista dos Tribunais, 2003. p. 93.

O direito à privacidade, por ser de primeira geração por estar vinculado diretamente à personalidade humana, atribuiu ao indivíduo a proteção da intimidade e da vida privada, como um dos fundamentos da dignidade da pessoa humana, apresentada pelo texto constitucional de 1988 como um estabilizador do Estado Democrático de Direito. Laura Mendes ressalta que os ordenamentos jurídicos de diversos países passaram a tutelar, não apenas a privacidade, mas expressamente os dados pessoais de seus cidadãos, por entenderem que tais dados constituem uma projeção da personalidade do indivíduo, e merecem tutela constitucional[76]. Danilo Doneda possui uma preocupação especial com o protagonismo da informação pessoal para a atualidade e a tutela dos direitos fundamentais dos titulares da informação[77]. Inicialmente ele trata dos dados pessoais e os direitos envolvidos, e ressalta a importância do direito à privacidade como protagonista das discussões jurídicas.

Diante disso, a proteção da privacidade na sociedade da informação deve ser repensada a partir da proteção de dados pessoais, pois é necessário o indivíduo ter meios necessários à construção e consolidação de uma esfera privada própria, de modo que a tutela da privacidade cumpra um papel positivo e permita a comunicação e relacionamento do indivíduo[78].

Nessa esteira, entende-se que há um diálogo entre o direito à privacidade e à proteção dos dados pessoais à luz da necessidade de se considerar a proteção de dados pessoais como um direito da personalidade autônoma[79]. Com efeito, diante do apresentado, é possível afirmar que o direito à privacidade deve se inserir nesta tutela dinâmica, porém quanto ao direito à proteção de dados pessoais, este deve ser interpretado como um direito autônomo, um novo direito da personalidade, não associado como uma evolução histórica do direito à privacidade. Pode haver algum intercâmbio, mas não uma associação direta, pois o direito à proteção de dados está atrelado ao conceito de dado pessoal[80].

---

[76] BESSA, Leonardo Roscoe. *O consumidor e os limites dos bancos de dados de proteção ao crédito.* São Paulo: Editora Revista dos Tribunais, 2003. P. 18.

[77] Isso decorre da popularização da internet e das tecnologias de transmissão e armazenamento de informações, que torna mais acessível e menos custosa a troca de informação pessoal, e ocasiona a exposição da informação pessoal no meio digital. DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* São Paulo: Thomson Reuters, 2019. p. 35.

[78] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. São Paulo: Thomson Reuters, 2019. p. 45.

[79] BIONI, Bruno Ricardo. *Proteção de Dados Pessoais*: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021. p. 138.

[80] BIONI, Bruno Ricardo. *Proteção de Dados Pessoais*: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021. p. 140.

Nesse sentido, houve um grande movimento no Congresso Nacional para incluir o direito à proteção de dados pessoais no rol de direitos fundamentais, o que fez gerar a construção do Projeto de Emenda Constitucional nº 17 de 2019. Tal projeto foi aprovado nos dois turnos pelo Senado no dia 20 de outubro de 2021 e encaminhado para promulgação. Com a aprovação da PEC 17/2019 e posterior promulgação (fevereiro de 2022) da correspondente EC 115/22, a discussão sobre a conveniência e oportunidade da inserção de um direito à proteção de dados pessoais na CF, ficou, de certo modo, superada. De acordo com o texto da EC 115, foi acrescido o inciso LXXIX ao artigo 5º, CF, que transformou a proteção de dados pessoais em direito fundamental, o qual dispõe que "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais" (Incluído pela Emenda Constitucional nº 115, de 2022)[81].

Destaca-se que o STF já reconhecia em decisões a proteção de dados como um direito fundamental implícito, o que extrai todas as consequências atinentes à tal condição. Porém, a sua positivação formal de forma expressa na CF, possui uma carga positiva muito maior, devido a uma série de lacunas regulatórias. Em razão disso, com o reconhecimento do referido direito fundamental, passa a inexistir uma "zona livre" de proteção dos dados pessoais na ordem jurídica brasileira[82].

Assim, em sua acepção formal, a importância do reconhecimento da proteção de dados pessoais como um direito fundamental ou direito humano decorre do fato de que os direitos fundamentais podem ser imediatamente aplicáveis, além de vincular diretamente, sem lacunas, todos os poderes e atores estatais, possuir eficácia nas relações entre particulares, bem como estabelecer limites materiais ao poder de reforma constitucional por meio de mecanismos de controle de legitimidade constitucional, o que permite a construção de um regime jurídico (garantias) que garanta robustez a proteção do cidadão, titular deste direito, frente ao Estado. Já em sentido material, as normas de direitos fundamentais apresentam um conteúdo jurídico de extrema relevância para indivíduos e para o interesse coletivo.

---

[81] SARLET, Ingo Wolfgang. A EC 115/22 e a proteção de dados pessoais como Direito Fundamental I. *Consultor Jurídico*, 2022. Disponível em: https://www.conjur.com.br/2022-mar-11/direitos-fundamentais-ec-11522-protecao-dados-pessoais-direito-fundamental. Acesso em: 14, set 2022.

[82] SARLET, Ingo Wolfgang. A EC 115/22 e a proteção de dados pessoais como Direito Fundamental I. *Consultor Jurídico*, 2022. Disponível em: https://www.conjur.com.br/2022-mar-11/direitos-fundamentais-ec-11522-protecao-dados-pessoais-direito-fundamental. Acesso em: 14, set 2022.

3.1.1 Do novo conceito e alcance do direito à Privacidade e Intimidade trazidos pela LGPD

Conforme visto acima sobre a evolução histórica do direito à privacidade até a transformação da proteção de dados pessoais como direito fundamental e autônomo, é importante abordar, também, sobre os novos conceitos e alcance do direito à privacidade e da intimidade trazidos ao longo do tempo e pela LGPD, que geram um conceito mais amplo de dado pessoal e trazem consequências ao tratamento de dados pessoais.

Com o avanço da tecnologia e o mundo digitalizado, novas dimensões para a coleta de dados foram expostas, o que faz aumentar a consciência da impossibilidade do segredo, tendo em vista a publicização mundializada de fatos, quebrando o conceito tradicional da privacidade. Por isso, é possível afirmar que o problema não está mais limitado ao indivíduo, mas se expande ao coletivo, na certeza de que a proteção não está mais na sequência pessoa-informação-sigilo, mas sim, na sequência pessoa-informação-circulação-controle, posto que o titular do direito não mais pode interromper o fluxo das informações que lhe digam respeito, mas, somente, "[...] exigir formas de circulação controlada"[83].

Logo, a privacidade, hoje, assumiu novos contornos e visa a proteção e prevenção da exposição de informações não consentidas, independentemente da propriedade, a demandar a atuação do Estado contra ingerência na vida privada, a partir de dados coletados e tratados, inclusive pelo próprio Poder Público. A privacidade e a informação pessoal, com a tecnologia e mudanças sociais e políticas, irão se relacionar, erigindo o controle da informação como poder dentro da sociedade e objeto de tutela legal, que José Alfredo de Oliveira Baracho viria a identificar como um novo direito, decorrente da redefinição de direitos anteriores, para adaptá-los ao contexto social informatizado.

Já em relação ao direito à intimidade, esse surge da modernidade como resposta jurídica às exigências éticas e aos problemas políticos na conjuntura histórica. Ocorre que mesmo sendo possível diferenciar essas esferas, tanto a expressão vida privada quanto o termo intimidade pretendem o mesmo objetivo: garantir a dignidade da pessoa humana de forma mais ampla possível, considerando a complexidade das situações subjetivas para o alcance da liberdade e construção da consciência do poder de autodeterminação.

---

[83] RODOTÁ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 93.

Para isso, é necessário considerar as diversas noções atribuídas à vida privada, segundo a cultura comum a cada grupo, num dado momento histórico, em relação ao objetivo perseguido para intromissão na vida privada. Assim como o princípio da dignidade humana, o conceito de privacidade não prescinde da contextualização histórica, para, então, se alcançar a consciência de que a proteção da intimidade não está desassociada do futuro, mas antes, deve considerar a efetividade da dignidade da pessoa humana "[...] com sua vinculação à livre autodeterminação de toda pessoa para atuar no mundo que a rodeia"[84].

Nesse novo cenário, a tecnologia deixou de ser mera situação de fato, isolada, para ser um vetor condicionante da sociedade, e, por conseguinte, assumir o centro de gravidade do direito à privacidade, no universo de multiplicidade de direitos envolvidos, na atual sociedade informacional[85]. Heinrich Hubmann e Heinrick Henkel apresentam três círculos na Teoria dos Círculos Concêntricos: a circunferência mais externa, limítrofe à sociedade, porém, de maior amplitude, é a da privacidade. Nessa esfera tem-se o âmbito das relações interpessoais, da imagem, dos costumes e dos hábitos. A circunferência intermediária é a da intimidade, que abarca o sigilo e as restrições de informações pessoais, relacionadas à família, amigos ou trabalho. Na circunferência interior está o segredo, reservado à psique humana, e por isso inacessíveis a outros, a não ser se desvelado pela vontade do próprio individuo, mas, nem por isso, passível de publicização[86].

Os arts. 5º, LX, e 93, IX, da Constituição Federal da República de 1988 garantem a publicidade dos atos judiciais, entretanto, garantem restrições nas hipóteses de violação à intimidade ou interesse social, a ser delineada ou conformada por lei. Os dispositivos que contenham uma reserva de lei restrita reconhecem a garantia de determinado âmbito de proteção, bem como uma norma de autorização de restrições que permita ao legislador

---

[84] BARACHO, José Alfredo de Oliveira. *Direito Processual Constitucional*: aspectos contemporâneos. Belo Horizonte: Fórum, 2006. p. 108.

[85] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

[86] GONÇALVES, Diego; RODRIGUES, Bruno Aloy. Os desafios à preservação da intimidade e da privacidade no âmbito virtual: um debate à luz das teorias dos círculos concêntricos e do mosaico. *In*: SEMINÁRIO INTERNACIONAL DEMANDAS SOCIAIS; MOSTRA INTERNACIONAL DE TRABALHOS CIENTÍFICOS, 11., 2018, [*S. l.*]. *Anais*... [*S. l.*]: UNISC, 2018. Disponível em: https://online.unisc.br/acadnet/anais/index.php/sidspp/article/view/18778/119261205. Acesso em: 16 jun. 2021.

estabelecer os limites do âmbito de proteção constitucionalmente assegurados[87]. É o caso do art. 189 do Código de Processo Civil, que ao trazer em seu *caput* a garantia da publicidade processual, limitou o direito fundamental por meio da instituição do segredo de justiça aos processos que exijam o interesse público ou social; que versem sobre relações de família; que constem dados protegidos pelo direito constitucional à intimidade e que versem sobre arbitragem com cláusula de confidencialidade. Por isso, o processo não tramita em segredo, às portas fechadas. A ele é conferido as mesmas garantias do devido processo constitucional, além da preservação da intimidade dos litigantes pela indevida ou desnecessária exposição pública, sendo mais pertinente a expressão publicidade restrita, tal como previsto constitucionalmente.

Nesse contexto, a lei restritiva deve expressar o âmbito de proteção do direito a ser reprimido, decorrer de autorização constitucional, com o escopo de salvaguardar outros interesses constitucionalmente protegidos, apresentando-se, ao mesmo tempo, adequada, necessária e proporcional ao fim proposto. E, em todas as hipóteses, garantir à norma restringida a eficácia de seu núcleo essencial. Assim, as garantias fundamentais, assim como suas restrições, possuem um processo de construção evolutivo e dinâmico, que se baseia nas modificações históricas, sem admitir, contudo, a relativização de preceitos fundamentais diante de meras contingências. Com efeito, a mesma dinamicidade que é atribuída às garantias e aos núcleos essenciais dos direitos fundamentais, tendo em conta a evolução dos fatos sociais, autoriza a consideração de normas restritivas infraconstitucionais, que correspondam dinâmica e evolutivamente ao mesmo contexto histórico de aplicação do direito fundamental, a demandar uma proposição restritiva legal consentânea à realidade, motivo em que se torna mais difícil ao Poder Público ponderar os direitos fundamentais e normas restritivas que colidem entre si, o que será melhor analisado a seguir.

3.1.2 Ponderação dos princípios da Publicidade, Privacidade e Intimidade

A publicidade é um dos princípios mais exercidos pela Administração Pública, um dos princípios mais norteadores do Estado Democrático de Direito, que confere transparência e propicia o controle de legalidade e legitimidade dos atos da Administração

[87] ARAÚJO, Eugênio Rosa de. Uma introdução aos direitos fundamentais. *Revista da SJR*, Rio de Janeiro, n. 25, p. 315-352, 2009. Disponível em: https://www.jfrj.jus.br/sites/default/files/revista-sjrj/arquivo/17-341-2-pb.pdf. Acesso em: 16 jun. 2022.

Pública. É um princípio que constitui em um dever da administração e se complementa com o direito à informação do cidadão. A CRFB apresenta o princípio da publicidade nos artigos 5º, LX[88], 37[89] e 93, IX[90]. O princípio da publicidade dos atos processuais está disposto no art. 93, X, CRFB, as quais são normas de observância obrigatória no Estatuto da Magistratura e complementam o direito ao devido processo legal, por possibilitar o direito ao contraditório e ampla defesa e atuam como pressupostos para o controle das decisões do Poder Judiciário e a prestação jurisdicional real e efetiva[91].

Contudo, em relação à importância da publicidade dos atos processuais e das decisões judiciais, sua observância encontra limites no interesse público à intimidade e à privacidade do cidadão. A formação desse círculo vicioso (exposição, acesso, revelação) decorre da dicotomia das garantias fundamentais da publicidade dos atos do processo e da privacidade, aparentemente conflituosos, mas complementares e fundamentais para a efetivação do devido processo constitucional. Assim, devem ser analisados os princípios constitucionais da publicidade processual e da privacidade, ambos direitos fundamentais, não como direitos e garantias individuais absolutos, mas relativos em função do indivíduo, de acordo com as relações interpessoais e sociais em concreto, de modo a potencializar a tutela jurisdicional em observância ao princípio da dignidade humana, esse sim, hierarquicamente superior.

Dessa forma, aplicar o princípio da proporcionalidade diante do caso em concreto, busca fazer com que nenhuma restrição a direitos fundamentais tome dimensões desproporcionais. Seria uma restrição às restrições pelo exame da adequação, da necessidade e da proporcionalidade em sentido estrito, para se chegar ao princípio de

---

[88] Art. 5º, CRFB. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
[...]
LX - a lei só poderá restringir a publicidade dos atos processuais quando a defesa da intimidade ou o interesse social o exigirem;

[89] Art. 37, CRFB. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência [...];

[90] Art. 93, CRFB. Lei complementar, de iniciativa do Supremo Tribunal Federal, disporá sobre o Estatuto da Magistratura, observados os seguintes princípios:
[...]
IX - todos os julgamentos dos órgãos do Poder Judiciário serão públicos, e fundamentadas todas as decisões, sob pena de nulidade, podendo a lei limitar a presença, em determinados atos, às próprias partes e a seus advogados, ou somente a estes, em casos nos quais a preservação do direito à intimidade do interessado no sigilo não prejudique o interesse público à informação;

[91] PADILHA, Rodrigo. *Direito Constitucional*. 5. ed. Rev. Ampl. Rio de Janeiro: Forense, São Paulo: Método, 2018. p. 805.

maior incidência ao caso, ainda que sejam considerados conjuntamente, a partir de concessões mútuas[92].

Contudo, a partir do que foi dito, é necessário fazer a seguinte pergunta? Na prática judiciária, quem seria o responsável a aplicar o princípio da proporcionalidade nos casos em que os direitos fundamentais da publicidade e privacidade conflitem entre si? Na busca do equilíbrio entre os ideais da privacidade e da publicidade dos atos processuais, cabe, hoje, ao julgador, ao magistrado, o sopesamento dos valores inerentes à pessoa humana. Contudo, o magistrado não seria a pessoa mais adequada a efetuar tal análise. Por mais que a aplicação do exame de adequação, da necessidade e da proporcionalidade seja uma forma válida e relevante ao Poder Judiciário conseguir restringir com mais efetividade as colisões entre princípios, por tratar-se de princípios que visam a privacidade e intimidade de um cidadão, o magistrado não é a pessoa mais correta a aplicar esse sopesamento, e sim, o próprio titular do dado exercendo seu direito de Autodeterminação Informativa.

Em outras palavras, ao se tratar de dados pessoais processuais que correspondem à privacidade e intimidade da parte, cabe ao próprio titular fazer o controle dos seus dados pela utilização desses métodos de ponderação analisando se determinado dado pessoal, caso publicizado, violará ou não sua privacidade e intimidade. A forma como isso se daria será visto em tópico específico do próximo capítulo. Portanto, é possível concluir que é possível afirmar que a publicidade dos atos processuais garante o Estado Democrático de Direito e são importantes para fornecer transparência da atividade jurisdicional ao cidadão. Contudo, a não publicização de informações pessoais nos processos judiciais não importa na violação desse princípio. Ao contrário, a ocultação para o público dos dados pessoais dos sujeitos do processo, pelas vias de segredo de justiça, ou pelos métodos de anonimização e pseudonimização, os quais serão vistos no último capítulo, otimizará tanto o princípio da publicidade, como o princípio da privacidade.

A otimização da garantia da publicidade, com a transparência dos atos processuais em todos os procedimentos judiciais, até mesmo aqueles classificados como segredo de justiça, favorece a fiscalização pública, sem que daí sobrevenha prejuízo ao princípio da privacidade dos sujeitos do processo, já que a ocultação externa das informações pessoais dos litigantes impossibilitará – ou pelo menos dificultará – a vinculação dos sujeitos do processo aos fatos narrados na lide, garantindo-lhes, assim, a proteção da vida privada e

[92] ALEXY, Robert. *Teoria dos direitos fundamentais*. Trad. Virgílio Afonso da Silva. 2. ed. São Paulo: Malheiros, 2017.

intimidade. Sob o mesmo raciocínio, a otimização do princípio da privacidade pode se dar pela exposição de todos os atos do processo, desde que relativizada a publicidade, com a vedação de acesso público aos dados pessoais dos litigantes, garantindo à coletividade a fiscalização dos atos decisórios.

3.2 DA LEGITIMIDADE DO PODER JUDICIÁRIO NA APLICAÇÃO DA LGPD E DAS RESOLUÇÕES NORMATIVAS CRIADAS PELO CNJ PARA SUA ADEQUAÇÃO

A Lei Geral de Proteção de Dados é aplicada não apenas no âmbito privado e às pessoas naturais e jurídicas de direito privado, mas também às de direito público, art. 3º, da LGPD. O termo "Poder Público" é definido de forma ampla e inclui órgãos ou entidades dos entes federativos (União, Estados, Distrito Federal e Municípios), art. 1º, parágrafo único, LGPD. A lei faz menção ao artigo 1º da Lei 12.527/2011 (Lei de Acesso à Informação) para definir seu campo de aplicação em relação ao Poder Público, sendo que o artigo 1º, parágrafo único, inciso I desta lei prevê sua incidência não só aos órgãos públicos integrantes da Administração Direta do Poder Executivo, como também aos órgãos integrantes do "Legislativo, incluindo as Cortes de Contas, Judiciário e do Ministério Público".

Também se incluem no conceito de Poder Público: (i) os serviços notariais e de registro (art. 23, §4º); e (ii) as empresas públicas e as sociedades de economia mista (art. 24), neste último caso, desde que (ii.i.) não atuem em regime de concorrência; ou (ii.ii) operacionalizem políticas públicas, no âmbito da execução destas. Os tratamentos de dados pessoais realizados por essas entidades e órgãos públicos devem observar as disposições da LGPD previstas no capítulo IV da lei e ressalvadas as exceções previstas no art. 4º, da lei. Dessa forma, uma vez que a LGPD fez questão de fornecer legitimidade à Administração Pública do Poder Público em aplicar as normas previstas da lei, o Poder Judiciário tem legitimidade e o dever de se adequar à lei. Para isso, o Conselho Nacional de Justiça editou várias resoluções normativas com o intuito de adequar os Tribunais às normas da LGPD e uniformizar a matéria no âmbito dos seus órgãos.

Em 20 de agosto de 2020 o Conselho Nacional de Justiça publicou a Recomendação nº 73/2020, que "Recomenda aos órgãos do Poder Judiciário brasileiro a adoção de medidas preparatórias e ações iniciais para adequação às disposições contidas

na Lei Geral de Proteção de Dados – LGPD."[93]. A recomendação, que não alcança o Supremo Tribunal Federal, sugere a disponibilização de informações precisas, sobre a coleta de dados, incluindo a base legal, finalidade e medidas de segurança da informação, nos sítios eletrônicos dos respectivos tribunais, dispondo, ainda, sobre a instituição de um grupo de trabalho, por meio da Portaria nº 63/2019[94], mais tarde revogada pela Portaria nº 212/2020[95], que instituiu grupo de trabalho "destinado a elaboração de estudos e propostas, voltadas à adequação dos tribunais à Lei Geral de Proteção de Dados e dá outras providências".

Em 12 de janeiro de 2021, o Conselho Nacional de Justiça publicou a Resolução nº 363/2021, que, a partir das conclusões apresentadas pelo grupo de trabalho formado pela Portaria 212/2020, "estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais"[96], à exceção do Supremo Tribunal Federal, consignando a necessidade de criação de um Comitê Gestor de Proteção de Dados Pessoais (CGPD), responsável pelo processo de implementação da LGPD, em cada tribunal, com a designação de um encarregado pelo tratamento de dados, na forma prevista no art. 41 da lei.

A referida resolução normativa determina, ainda, a formação de "Grupo de Trabalho Técnico de caráter multidisciplinar para auxiliar nas funções junto ao encarregado pelo GT, composto, entre outros, por servidores da área de tecnologia, segurança da informação e jurídica"[97], cabendo ao órgão judicial informar a base legal que legitima o tratamento de dados, as obrigações dos controladores e direitos dos

---

[93] CONSELHO NACIONAL DE JUSTIÇA. Recomendação nº 73, de 20/08/2020. Recomenda aos órgãos do Poder Judiciário brasileiro a adoção de medidas preparatórias e ações iniciais para adequação às disposições contidas na Lei Geral de Proteção de Dados – LGPD. Brasília, DF: CNJ, 2020. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3432. Acesso em: 16 jun. 2022.

[94] CONSELHO NACIONAL DE JUSTIÇA. Portaria nº 63 de 26/04/2019. Institui Grupo de Trabalho destinado à elaboração de estudos e propostas voltadas à política de acesso às bases de dados processuais dos tribunais e dá outras providências. Brasília, DF: CNJ, 2019. Disponível em: https://atos.cnj.jus.br/atos/detalhar/2890. Acesso em: 16 jun. 2022.

[95] CONSELHO NACIONAL DE JUSTIÇA. Portaria nº 212 de 15/10/2020. Institui Grupo de Trabalho destinado à elaboração de estudos e de propostas votadas à adequação dos tribunais à Lei Geral de Proteção de Dados e dá outras providências. Brasília, DF: CNJ, 2020. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3520. Acesso em: 16 jun. 2022.

[96] CONSELHO NACIONAL DE JUSTIÇA. Resolução nº 363 de 12/01/2021. Estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais. Brasília, DF: CNJ, 2021. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3668. Acesso em: 16 jun. 2022.

[97] CONSELHO NACIONAL DE JUSTIÇA. Resolução nº 363 de 12/01/2021. Estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais. Brasília, DF: CNJ, 2021. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3668. Acesso em: 16 jun. 2022.

titulares de dados, a identificação precisa do encarregado e a implementação de medidas de segurança para proteção e prevenção de situações acidentais ou ilícitas no manuseio de dados.

Enquanto a revogada Portaria nº 63/2019[98] instituiu grupo de trabalho para apresentação de uma proposta coesa de observância geral, por meio de um relatório a ser apresentado ao Comitê Permanente de Tecnologia e Infraestrutura do Conselho Nacional de Justiça, a Portaria nº 212/2020 do Conselho Nacional de Justiça, que a sucedeu, previu a elaboração de estudo que permitisse a cada tribunal, no âmbito de sua atuação administrativa ou judicial, a implementação de ações imediatas para melhor adequação à LGPD, não obstante as dificuldades de consenso e implementação de regras em todos os tribunais brasileiros.

Isso importa dizer que cada Comitê de Proteção de Dados Pessoais, instituído em cada tribunal, dará a interpretação que lhe parecer mais adequada aos preceitos normativos da LGPD, de acordo com os critérios, objetivos e alcance do tratamento dos dados pessoais, tendo em conta suas funções administrativas e jurisdicionais, ainda que a atuação jurisdicional corresponda à mesma em todo território nacional, como órgão de jurisdição uno, em atenção ao princípio *una lex, una jurisdictio*[99].

Já nos termos da Resolução nº 363/2021, cada tribunal estará autorizado a implementar medidas de segurança técnicas, nos termos do art. 46 e seguintes da Lei nº 13.709/2018, o que, por força do inciso XI do art. 1º da referida resolução, equivale dizer que os tribunais poderão contar, ainda, com diretrizes da ANPD, de acordo com o estado da tecnologia atual, mormente em vista do tratamento de dados sensíveis e os princípios que regem a LGPD. Determinou, ainda, que por força do art. 25 da LGPD, no exercício da função pública jurisdicional, o Judiciário deve manter todos os dados sob sua guarda em formato interoperável e estruturado para uso compartilhado, o que pressupõe que todas as medidas de segurança, técnicas e administrativas, adotadas pelos tribunais do Estado Brasileiro devem estar no mesmo nível máximo de operacionalização para "proteger os dados pessoais de acessos não autorizados e de situações acidentais ou

---

[98] CONSELHO NACIONAL DE JUSTIÇA. Portaria nº 63 de 26/04/2019. Institui Grupo de Trabalho destinado à elaboração de estudos e propostas voltadas à política de acesso às bases de dados processuais dos tribunais e dá outras providências. Brasília, DF: CNJ, 2019. Disponível em: https://atos.cnj.jus.br/atos/detalhar/2890. Acesso em: 16 jun. 2022.

[99] PELLEGRINO, Maria Cristina Conde. *DA MIHI DATA, DABO TIBI JUS*: o tratamento de dados pessoais no âmbito do processo judicial eletrônico brasileiro, à luz da Lei Geral de Proteção de Dados' 13/07/2021 147 f. Dissertação (Mestrado em Instituições Sociais, Direito e Democracia) - UNIVERSIDADE FUMEC, Belo Horizonte Biblioteca Depositária: FCH, 2021.

ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, nos termos do art. 46 e seguintes da LGPD"[100].

Com efeito, diante das resoluções criadas pelo CNJ, é possível afirmar que não há regulamentação de alcance geral sobre os meios técnicos mais adequados e consentâneos com a melhor tecnologia voltada à segurança do sistema e à prevenção de incidentes de acesso não autorizado. Pelo contrário, limitam-se a transferir essa responsabilidade a cada um dos tribunais brasileiros, sem uma padronização e uniformização. Além do mais, não tratam de métodos de restrição ao livre acesso de terceiros aos milhares de dados pessoais expostos nos processos judiciais eletrônicos, decisões judiciais, jurisprudência e demais serviços de divulgação, pautando-se as resoluções em obrigações genéricas previstas na LGPD. Assim também, ao ser recomendada a divulgação de informações no sítio eletrônico das cortes judiciais (à exceção do Supremo Tribunal Federal), quanto à forma e às obrigações a serem adotadas no tratamento de dados, inexiste a recomendação ou informação voluntária sobre quais providências foram efetivadas e como foram cumpridas.

Por tudo isso, é possível afirmar que as resoluções criadas pelo CNJ ainda não suprem uma adequação efetiva do Judiciário às normas da LGPD. Portanto, é possível concluir que a LGPD fez questão de fornecer legitimidade e o dever do Poder Judiciário em aplicar as regras previstas em lei. A criação pelo CNJ de várias resoluções como tentativa de melhor adequar os tribunais à essas normas, demonstra que o Judiciário possui interesse em cumprir a lei e está caminhando para que cada dia se adeque mais a ela. Contudo, possuir legitimidade e criar resoluções para adequação padronizada não quer dizer que estão aplicando a LGPD de forma eficaz e eficiente, pois ainda possuem muitos dados pessoais expostos em seus sistemas e sem nenhuma proteção e regulamentação para isso. Além do mais, o Poder Público possui uma cultura mais atrasada ao manuseio de novas tecnologias e à adaptação ao mundo digital, o que torna esse processo de adequação muito mais lento em comparação ao âmbito privado, deixando os órgãos vulneráveis, alvos de vários ataques maliciosos e sujeitos a enfrentarem vários problemas e desafios para essa adequação, os quais serão vistos a seguir.

---

[100] CONSELHO NACIONAL DE JUSTIÇA. Resolução nº 363 de 12/01/2021. Estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais. Brasília, DF: CNJ, 2021. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3668. Acesso em: 16 jun. 2022.

3.3 LEI DO PROCESSO JUDICIAL ELETRÔNICO: DA ESTRUTURA NORMATIVA AO ACESSO DOS DADOS PESSOAIS

A urgência do Judiciário em atender os objetivos constitucionais que exigem a era digital foi considerável, como prover um amplo acesso dos cidadãos aos tribunais, uma razoável duração do processo judicial, bem como o respeito aos princípios da publicidade processual. Pensando nessa exigência de um Judiciário mais acessível e ágil, foi criado uma estrutura legal/informacional para o Processo Judicial Eletrônico (PJe) e o Diário de Justiça Eletrônico (DJe), ou seja, foi determinado pela lei a transição dos procedimentos dos tribunais brasileiros de uma arcaica massa de documentos de papel para bancos de dados virtuais.

Assim, foram instituídos pela lei 11.419/2006, o PJE e DJE, que determinou o uso de meio eletrônico na tramitação de processos judiciais que englobam todas as decisões judiciais, transmissão de peças processuais das partes e comunicação de atos dos tribunais. A lei abrange os processos civis, penais e trabalhistas, em qualquer grau de jurisdição, inclusive os juizados especiais. Logo, toda a tramitação processual no sistema judiciário à luz da referida Lei nº 11.419, de 19 de dezembro de 2006, deve ser por meio de sistema computacional. Entre as melhorias almejadas pela lei, pode-se citar:

- Celeridade na tramitação processual;
- Razoável duração do processo;
- Facilitar acesso à justiça;
- Promover transparência da evolução processual para o cidadão em litígio;
- Aprimorar a gestão do arquivo legado de processos já finalizados que eram realizados todos em papel, gerando diversas despesas como a manutenção de espaço físico para armazenamento de processos, rotinas de combate a umidade e fungos, controles de risco de incêndio e dificuldade de localização, entre outros.

Segundo dados do Conselho Nacional de Justiça (CNJ), disponível no relatório analítico “Justiça em números 2022”, ano-base 2021[101], o Poder Judiciário terminou em 2021 com 62 milhões de ações judiciais em andamento, que é a diferença entre os 77,3

[101] CONSELHO NACIONAL DE JUSTIÇA. Justiça em Números 2022: Judiciário julgou 26,9 milhões de processos em 2021. Disponível em https://www.cnj.jus.br/justica-em-numeros-2022-judiciario-julgou-269-milhoes-de-processos-em-2021/#:~:text=Justi%C3%A7a%20em%20N%C3%BAmeros%202022%3A%20Judici%C3%A1rio,processos%20em%202021%20%2D%20Portal%20CNJ&text=O%20Poder%20Judici%C3%A1rio%20concluiu%2026,solucionados%20em%20rela%C3%A7%C3%A3o%20a%202020. Acesso em: 21 Nov. 2022.

milhões de processos em tramitação e os 15,3 milhões (19,8%) sobrestados ou em arquivo provisório, aguardando definição jurídica futura. Dos 90 órgãos do Judiciário, 44 aderiram integralmente ao Juízo 100% digital, o que abrange 67,7% das serventias judiciais. Segundo o CNJ, nessas unidades, todos os atos processuais podem ser praticados por meio eletrônico e remoto, inclusive audiências e sessões de julgamento, o que fez com que, segundo o anuário, os processos eletrônicos tivessem uma redução média de três anos e quatro meses no tempo de tramitação, o que pode representar quase um terço dos prazos registrados nos processos físicos, que giram em torno de nove anos e nove meses[102]. Assim, verifica-se que a vinda do processo judicial eletrônico e a adoção de mecanismos tecnológicos para cumprir os objetivos constitucionais da lei, foram essenciais para o Judiciário conseguir com mais celeridade dar vazão aos milhões de processos existentes.

Por outro lado, diante dessa informatização processual, com a vinda do Processo Judicial Eletrônico, os dados pessoais das partes se tornaram mais expostos na rede mundial de computadores, uma vez que seus nomes e iniciais são indexadas por mecanismos de buscas e, também, são passíveis de se tornarem identificadas pelos sistemas de *Big Data Analytics*, mesmo em processos sob sigilo de justiça. Além disso, os operadores do direito, advogados, que recebem e tratam um conjunto de dados pessoais e dados pessoais sensíveis estão vulneráveis no sentido de não terem o treinamento necessário e nem usarem ferramentas adequadas para a proteção desses dados[103].

Assim, observa-se que a informatização da justiça apresenta aspectos positivos, entretanto, como efeito colateral, surge o risco de extrema exposição das partes processuais, atingindo, dessa forma, os direitos da personalidade, imagem, honra, reputação, privacidade, que são direitos fundamentais garantidos constitucionalmente. Nesse sentido, é importante destacar alguns dispositivos da Lei do Processo Eletrônico que tratam da publicidade e acesso dos atos processuais, e consequentemente, acesso a todos esses dados pessoais:

> Art. 4º Os tribunais poderão criar Diário da Justiça eletrônico, disponibilizado em sítio da rede mundial de computadores, para publicação de atos judiciais e

[102] CONSELHO NACIONAL DE JUSTIÇA. Justiça em Números 2022: Judiciário julgou 26,9 milhões de processos em 2021.

[103] OLIVEIRA, Frank Ned Santa Cruz de. *Gestão de riscos no direito fundamental à privacidade de dados pessoais no Processo Judicial Eletrônico* / Diário de Justiça Eletrônico. 2020., 136 f., il. Dissertação (Mestrado Profissional em Computação Aplicada) - Universidade de Brasília, Brasília, 2020.

administrativos próprios e dos órgãos a eles subordinados, bem como comunicações em geral.
[...]
§ 2º A publicação eletrônica na forma deste artigo substitui qualquer outro meio e publicação oficial, para quaisquer efeitos legais, à exceção dos casos que, por lei, exigem intimação ou vista pessoal.
[...]
Art. 8º Os órgãos do Poder Judiciário poderão desenvolver sistemas eletrônicos de processamento de ações judiciais por meio de autos total ou parcialmente digitais, utilizando, preferencialmente, a rede mundial de computadores e acesso por meio de redes internas e externas.
[...]
Art. 11. Os documentos produzidos eletronicamente e juntados aos processos eletrônicos com garantia da origem e de seu signatário, na forma estabelecida nesta Lei, serão considerados originais para todos os efeitos legais.
[...]
§ 6º Os documentos digitalizados juntados em processo eletrônico estarão disponíveis para acesso por meio da rede externa pelas respectivas partes processuais, pelos advogados, independentemente de procuração nos autos, pelos membros do Ministério Público e pelos magistrados, sem prejuízo da possibilidade de visualização nas secretarias dos órgãos julgadores, à exceção daqueles que tramitarem em segredo de justiça. (Incluído pela Lei nº 13.793, de 2019)
§ 7º Os sistemas de informações pertinentes a processos eletrônicos devem possibilitar que advogados, procuradores e membros do Ministério Público cadastrados, mas não vinculados a processo previamente identificado, acessem automaticamente todos os atos e documentos processuais armazenados em meio eletrônico, desde que demonstrado interesse para fins apenas de registro, salvo nos casos de processos em segredo de justiça. (Incluído pela Lei nº 13.793, de 2019)
[...]
Art. 12. A conservação dos autos do processo poderá ser efetuada total ou parcialmente por meio eletrônico.
[...]
§ 1º Os autos dos processos eletrônicos deverão ser protegidos por meio de sistemas de segurança de acesso e armazenados em meio que garanta a preservação e integridade dos dados, sendo dispensada a formação de autos suplementares.
§ 2º Os autos de processos eletrônicos que tiverem de ser remetidos a outro juízo ou instância superior que não disponham de sistema compatível deverão ser impressos em papel, autuados na forma dos arts. 166 a 168 da Lei nº 5.869, de 11 de janeiro de 1973 - Código de Processo Civil, ainda que de natureza criminal ou trabalhista, ou pertinentes a juizado especial.
§ 3º No caso do § 2º deste artigo, o escrivão ou o chefe de secretaria certificará os autores ou a origem dos documentos produzidos nos autos, acrescentando, ressalvada a hipótese de existir segredo de justiça, a forma pela qual o banco de dados poderá ser acessado para aferir a autenticidade das peças e das respectivas assinaturas digitais.
Art. 13. O magistrado poderá determinar que sejam realizados por meio eletrônico a exibição e o envio de dados e de documentos necessários à instrução do processo.
§ 1º Consideram-se cadastros públicos, para os efeitos deste artigo, dentre outros existentes ou que venham a ser criados, ainda que mantidos por concessionárias de serviço público ou empresas privadas, os que contenham informações indispensáveis ao exercício da função judicante.
§ 2º O acesso de que trata este artigo dar-se-á por qualquer meio tecnológico disponível, preferentemente o de menor custo, considerada sua eficiência.

Verifica-se nos dispositivos acima que a lei priorizou garantir mais acesso à justiça aos cidadãos e mais acesso aos atos e dados processuais pelos advogados e demais membros do judiciário, prevalecendo a garantia à publicidade dos atos processuais. Logo, a lei não se preocupou em trazer mais garantia de proteção aos milhões de dados pessoais expostos pelo Judiciário, como o nome das partes, profissão, dados relacionados a questões de saúde, cidade, estado, números de IPs, placas de veículos, endereços de imóveis, documentos que comprovam a vida financeira da parte, fotos, conversas íntimas, entre outros. Por esses motivos, é possível afirmar que a Lei do Processo Eletrônico não vai de encontro com as normas trazidas pela Lei Geral de Proteção de Dados Pessoais – LGPD.

Ainda nesse contexto de acesso, é importante mencionar que, segundo o site oficial da OAB, o Brasil é o país com a maior proporção de advogados por habitante do mundo. Ao todo, cerca de 1,3 milhão de advogados exercem regularmente a profissão entre 212,7 milhões de pessoas (IBGE). Proporcionalmente, há 1 advogado para 164 brasileiros residentes no país[104]. Ou seja, além dos magistrados, servidores dos Tribunais, estagiários, defensores públicos, promotores e demais membros do judiciário, todos esses advogados atuantes na profissão, que possuem um simples cadastro no PJE, tem acesso a todos os dados e documentos pessoais de uma parte em um processo judicial, mesmo não sendo patronos ou tendo qualquer vinculação no feito, com exceção dos processos em segredo de justiça.

Esse acesso facilitado desses membros a qualquer processo judicial, com exceção dos que tramitam em segredo de justiça, é preocupante, pois hoje, com apenas um *click* é possível baixar, em poucos minutos, todo o teor do processo, com todos os dados e documentos pessoais das partes, facilitando o compartilhamento desses dados a outros terceiros, e tornando as partes vulneráveis à atividades discriminatórias e alvo de práticas criminosas. Dito isso, é possível fazer as seguintes perguntas: por qual motivo é necessário todos esses membros que não possuem vínculo diretamente ao processo terem acesso aos dados e documentos pessoais das partes? A restrição do acesso a esses dados e documentos pessoais infringiria o direito fundamental da publicidade dos atos processuais?

---

[104] ORDEM DOS ADVOGADOS DO BRASIL. Brasil tem 1 advogado a cada 164 habitantes; CFOAB se preocupa com qualidade dos cursos jurídicos. Disponível em: https://www.oab.org.br/noticia/59992/brasil-tem-1-advogado-a-cada-164-habitantes-cfoab-se-preocupa-com-qualidade-dos-cursos-juridicos. Acesso em: 25 nov. 2022.

Em resposta, é possível afirmar que o direito fundamental da publicidade dos atos processuais é importante para evitar atos abusivos do poder público, oferecendo mais transparência à sociedade. No caso do Poder Judiciário, a transparência dos processos judiciais é ato essencial para a sociedade acompanhar as decisões do judiciário, seu entendimento e os atos praticados pelos magistrados como forma de ser evitado qualquer abuso ao poder, ou seja, não há o que questionar ou criticar o art. 5º, LX, da CF no que se refere à obrigatoriedade da publicidade dos atos processuais. Contudo, é importante trazer a reflexão de que em nenhum momento a Constituição Federal menciona a obrigatoriedade da publicidade dos dados e documentos pessoais das partes, sendo que ato processual é diferente de dado pessoal.

Logo, restringir o acesso aos dados e documentos pessoais processuais de membros internos e externos ao Judiciário que não possuem vínculo direto ao processo em litígio não infringiria os dispositivos da CF e demais leis infraconstitucionais que garantem a publicidade de atos processuais, pelo contrário, garantiria com muito mais efetividade os direitos fundamentais que envolvem a dignidade da pessoa humana, como a privacidade, intimidade e proteção de dados pessoais.

Inclusive, o próprio texto constitucional não atribui à publicidade processual um valor absoluto e incontrastável. Ao mesmo tempo em que proclama a publicidade de atos processuais como regra, a Constituição Federal a excepciona “quando a defesa da intimidade ou o interesse social o exigirem” (art. 5º, LX) e “em casos nos quais a preservação do direito à intimidade do interessado no sigilo não prejudique o interesse público à informação” (art. 93, IX).

Portanto, a Lei do Processo Eletrônico não vai de encontro com as regras previstas na Lei Geral de Proteção de Dados Pessoais, pelos seus objetivos centrais serem princípios que dificultam a proteção de dados pessoais, como garantir mais acesso à justiça aos cidadãos, mais acesso aos atos e dados processuais pelos advogados e demais membros do judiciário, promover mais transparência dos atos processuais, prevalecendo, portanto, como objetivo central da lei a garantia à publicidade e transparência dos atos processuais.

3.4 DA EXPOSIÇÃO DE DADOS PESSOAIS E SENSÍVEIS NOS PROCESSOS JUDICIAIS ELETRÔNICOS

Com o avanço de novas tecnologias, os dados pessoais dos indivíduos passaram a ficar cada vez mais expostos nas suas relações, sendo elas privadas ou públicas. No Poder Judiciário, a maior parte das informações são coletadas através do fornecimento pela própria parte que busca seus direitos pela via do processo judicial. O indivíduo, além de fornecer informações de caráter pessoal – nome, filiação, data de nascimento, sexo, estado civil, endereço residencial ou comercial, telefones, escolaridade e profissão, assinatura – vários outros documentos pessoais que dizem respeito à privacidade e intimidade da parte são fornecidos em processos litigiosos como forma de alcançar a prestação jurisdicional.

Esses dados pessoais devem receber proteção jurídica adequada. Não apenas a coleta, mas da mesma forma o armazenamento e o tratamento de dados necessitam de tutela jurídica. Afinal, trata-se de dados pessoais relativos à personalidade da pessoa, a aspectos da vida privada e que podem comprometer a imagem do indivíduo perante terceiros, sua moral e estrutura psíquica quando indevidamente utilizados ou tornados públicos. Nesse sentido, os processos judiciais são uma fonte inesgotável de dados pessoais e sensíveis titularizados pelos mais variados atores processuais (partes, testemunhas, vítimas, magistrados(as), advogados(as), auxiliares da justiça etc.) e terceiros. Ricardo Villas Bôas Cueva entende que:

> Os documentos em papel, anteriormente à digitalização e à possibilidade de acesso quase universal a uma enorme quantidade de dados, eram encobertos por uma 'obscuridade prática'. Coligir e processar informações era lento e dispendioso. Os autos judiciais eram considerados 'praticamente obscuros', de modo que não havia muito cuidado com a difusão e o tratamento de dados pessoais que pudessem ser deles extraída. Diversa é a situação quando tudo passa a ser digitalizado e acessível pela internet. A completa qualificação das partes, seus endereços, o nome de crianças menores, registros médicos, entre outras informações sensíveis, podem ser facilmente obtidos. O risco de exposição excessiva e de uso abusivo de informação passa a ser palpável e não se circunscreve à possibilidade de monitoramento do comportamento individual pelo Estado, especialmente diante da emergência de um novo paradigma econômico, a chamada economia digital, na qual certas empresas, com grande poder de mercado, têm como insumo básico os dados de seus consumidores, que são frequentemente mais lucrativos do que do que os bens ou serviços que oferecem[105].

[105] CUEVA, Ricardo Villas Bôas. A incidência da Lei Geral de Proteção de Dados Pessoais nas atividades do Poder Judiciário. *In*: CUEVA, Ricardo Villas Bôas; DONEDA, Danilo; MENDES, Laura Schertel (coord.). *Lei Geral de Proteção de Dados* (Lei n.º 13.709/2018): a caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020. E-book. Disponível em: https:// proview.thomsonreuters.com. Acesso em: 14 out. 2021. p. RB-13.3.

Ao se tratar do processo judicial eletrônico, para haver a jurisdição, a parte interessada na prestação jurisdicional será obrigada a fornecer seus dados pessoais para cumprir com as exigências procedimentais previstas em lei para o ajuizamento de uma ação, como indicar seu nome, prenome, estado civil ou a existência de união estável, profissão, número de inscrição no Cadastro de Pessoas Físicas, endereço eletrônico, o domicílio e a residência do autor e do réu, na forma imposta pelo art. 319 do Código de Processo Civil. Tratando-se de um dos requisitos para conhecimento da petição inicial, sob pena de indeferimento, tal como estabelecido no parágrafo único do art. 321 do Código de Processo Civil, antes da narrativa dos fatos, sobre os quais a norma legal irá incidir, o cidadão deve apresentar os dados pessoais para que o juiz diga o direito.

Nesse contexto, independentemente do consentimento do titular dos dados pessoais em sua atividade fim (judicante), o Judiciário manuseia, diariamente, incontáveis dados pessoais, bem como dados sensíveis, submetidos ao órgão público em razão da obrigação legal (art. 319, III). Assim é que, classificados pela LGPD, como controladores de dados, as cortes judiciais, de maneira geral, coletam, classificam, avaliam, armazenam, arquivam, entre outras atividades de tratamento de dados, assim agindo em cumprimento à ordem legal, exposta no Código de Processo Civil, de modo a justificar e legitimar o tratamento de dados pessoais e dados pessoais sensíveis, com base no inciso II do art. 7º[106], e na alínea "a" do inciso II do art. 11 da Lei nº 13.709, de 2018.

Assim, somente a partir da apresentação das informações pessoais dos litigantes exsurge a obrigação legal de o órgão judicante conhecer os fatos narrados que fundamentam o pedido judicial e, por conseguinte, o legítimo interesse público e obrigação legal de tratamento dos dados submetidos a julgamento, independentemente do consentimento do titular. Nesse sentido, é possível trazer alguns exemplos dessas informações pessoais expostas com frequência nos processos judiciais, fornecidas pelos próprios litigantes, com o intuito de cumprir com as determinações legais para o alcance da prestação jurisdicional. Em relação aos processos do âmbito cível, que envolvem as matérias de obrigação de fazer, danos materiais, morais, estéticos, contratos, dentre outras, são vários os dados e documentos pessoais expostos, como um contrato particular de compra e venda de veículo, onde todos os dados do automóvel estão disponíveis, fotos e conversas que envolvem a privacidade e intimidade da parte, laudos médicos e

[106] Art. 7º, LGPD O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
II - para o cumprimento de obrigação legal ou regulatória pelo controlador.

documentos que vislumbram todo o histórico de saúde da parte, documentos que demonstram a atual vida financeira da parte, assim como vários outros.

Já no âmbito previdenciário, na maior parte dos processos judiciais é possível acessar o extrato previdenciário do Cadastro Nacional de Informações Sociais (CNIS) contendo todos os dados importantes da vida contributiva das partes ao INSS, como todos os vínculos empregatícios que já exerceu com suas respectivas datas de início e saída, salários de benefício e contribuição, todos os benefícios já recebidos, como auxílio-doença, auxílio-acidente, salário à maternidade, salário-família, auxílio-reclusão, aposentadoria por invalidez, aposentadoria por idade, dentre outros. O acesso aberto a esses documentos faz com que as partes fiquem vulneráveis e sujeitas a atividades maliciosas, principalmente os idosos e pessoas com saúde fragilizada que estão esperando por muito tempo receber seu benefício pelo INSS, pois são alvos de ligações de terceiros maliciosos que se passam por funcionários do INSS e pedem uma entrada em dinheiro como forma de conseguirem a totalidade do seu benefício. Infelizmente, essa é uma realidade atual onde muitas fraudes nessa área estão acontecendo pela falta de proteção desses dados pessoais.

Já nos processos em que as partes solicitam os benefícios da justiça gratuita por serem hipossuficientes e cuja renda familiar é menor que 5 salários mínimos é necessário a juntada de documentos que comprovem sua renda familiar, como extratos bancários, imposto de renda, carteira de trabalho, dentre outros, documentos esses que expõem a vida patrimonial da parte, deixando-a, também, vulnerável à terceiros maliciosos ou às atividades discriminatórias praticadas por empresas privadas e públicas de crédito que possuem acesso a esses documentos através de seus setores jurídicos ou de parcerias com escritórios de advocacia ou até mesmo com o próprio judiciário.

Diante dessa quantidade de informações pessoais que estão expostas no Poder Judiciário e que são necessárias sua juntada ao processo judicial para o alcance da pretensão da parte, o Supremo Tribunal Federal, em recentes decisões, tem reconhecido a proteção de dados pessoais e a autodeterminação informativa como direitos fundamentais dotados de autonomia e oponíveis ao Poder Público. Inspirada por esse vetor interpretativo, a Corte, por exemplo, proibiu o compartilhamento de dados de usuários de telefonia com o IBGE (ADI 6.387 MC-Ref/DF, ADI 6.388 MC-Ref/DF, ADI 6.389 MC-Ref/DF, ADI 6.390 MC-Ref/DF, ADI 6.393 MC-Ref/DF, Tribunal Pleno, Rel. Min. Rosa Weber, DJe n. 270, 12 nov. 2020); rechaçou a criação de cadastro estadual de usuários(as) e dependentes de drogas (ADI 6.561 MC/TO, Tribunal Pleno, Rel. Min.

Edson Fachin, Dje n. 260, 29 out. 2020); estabeleceu condicionantes procedimentais e materiais à atuação de órgãos de inteligência (ADI 6.529 MC/DF, Tribunal Pleno, Rel. Min. Cármen Lúcia, DJe n. 249, 15 out. 2020); e vedou a produção de dossiês contra servidores(as) públicos(as) e professores(as) (ADPF 722 MC/DF, Tribunal Pleno, Rel. Min. Cármen Lúcia, DJe n. 255, 22 out. 2020)[107].

Embora esses julgados não cuidem especificamente do tratamento de dados pelo Poder Judiciário, eles são bastante ilustrativos do grau de importância que a proteção de dados de pessoas naturais assume no direito brasileiro contemporâneo, inclusive no contexto do desempenho de atividades estatais. Trata-se de um indicativo claro de que, em face de um quadro de mudanças tecnológicas profundas e aceleradas, a interpretação jurídica precisa ser atualizada para atender às novas demandas sociais.

3.5 DOS ATAQUES DE *HACKERS* E VAZAMENTO DE DADOS PESSOAIS NO PODER JUDICIÁRIO

Com a vinda em 2006 do processo eletrônico pela Lei nº 11.419/2006, e com o intuito principal de mais celeridade nos processos judiciais, todos os procedimentos processuais foram convertidos em plataformas computacionais, sob a gestão das cortes de justiça. Além da identificação nominal e relacionais de todos os sujeitos, o processo judicial congregou inúmeras informações, além de documentos sigilosos e estratégicos, vinculados às partes e à questão *sub judice*, também aportados na plataforma digital, acessível pela rede mundial de computadores.

Com o avanço e desenvolvimento tecnológico, a sociedade capitalista passou a ver os dados pessoais como o principal meio para o desenvolvimento de projetos comerciais, financeiros e industriais, criando perfis de consumidores e de eleitores, que permitem o controle de comportamento direto e indireto, além de concentrar informações pela padronização, de modo a garantir programas de buscas, compilações e dossiês informacionais. Assim, "[...] não é exagero dizer que os dados são o novo petróleo. Mais do que um insumo ou uma moeda, os dados correspondem a grandes fontes de poder

[107] CONSELHO NACIONAL DE JUSTIÇA. Tratamento de dados pessoais na consulta de jurisprudência: desafio e perspectivas. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2022/02/tratamento-dados-pessoais-consulta-jurisprudencia30-11-21.pdf. Acesso em: 29 nov. 2022.

econômico, social e político, na medida em que podem ser convertidos em informações úteis para os mais diversos propósitos."[108].

Pela facilidade da coleta de dados pessoais, esses podem ser considerados como ativos lucrativos e os dados acessados só representam um valor econômico se transformados em informação útil, pelo processamento e classificação, impondo-se o acesso simultâneo de dois recursos – dados e processamento[109]. Nesse sentido, se para serem valorados os dados precisam ser qualificados, quantificados e identificados, a exposição judicial de informações pessoais em bases digitais concentradas responde pela almejada valorização, já que dos autos do processo judicial podem ser extraídas informações correlacionadas, sistêmicas e objetivas, concernentes aos titulares dos dados pessoais, fazendo do Judiciário um dos maiores repositórios de dados pessoais classificados do país[110].

A preocupação com a questão foi enfrentada pelo Ministro do Superior Tribunal de Justiça, Ricardo Villas Bôas Cuevas, que, na análise da vulnerabilidade dos dados expostos em bases digitais, e diante da conclusão de que empresas lucram mais com informações de seus consumidores do que com os próprios produtos, trouxe para a ordem de discussão a necessidade de garantir a "opacidade às informações relativas às partes, a seus advogados e a terceiros eventualmente mencionados nos autos de processos judiciais, de modo a impedir o desvirtuamento da finalidade para o qual tais dados foram tratados"[111].

Não por outro motivo, desde a implementação do processo judicial eletrônico, onde os dados pessoais passaram a se tornar mais expostos, as cortes judiciais brasileiras já foram alvo de sete ataques cibernéticos em sete meses, assim como outros mais recentes, declaradamente exitosos, seja na captura de dados, seja na intervenção não autorizada ao sistema, o que provocou não só a coleta de informações pessoais, mas

---

[108] FRASÃO, Ana. Big Data e Aspectos Concorrenciais do Tratamento de Dados Pessoais. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (coord.). *Tratado de Proteção de Dados*. Rio de Janeiro: Forense, 2021. p. 536.

[109] FRASÃO, Ana. Big Data e Aspectos Concorrenciais do Tratamento de Dados Pessoais. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (coord.). *Tratado de Proteção de Dados*. Rio de Janeiro: Forense, 2021. p. 536

[110] PELLEGRINO, Maria Cristina Conde. *DA MIHI DATA, DABO TIBI JUS*: o tratamento de dados pessoais no âmbito do processo judicial eletrônico brasileiro, à luz da Lei Geral de Proteção de Dados' 13/07/2021 147 f. Mestrado em Instituições Sociais, Direito e Democracia Instituição de Ensino: UNIVERSIDADE FUMEC, Belo Horizonte Biblioteca Depositária: FCH, 2021.

[111] CUEVAS, Ricardo Villas Boas. Anonimização e Pseudonimização de Dados Pessoais no Processo Eletrônico. In: TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. O Direito Civil na era da Inteligência. São Paulo: Thomson Reuters Brasil, 2020. p. 255.

também o comprometimento do próprio sistema, de modo a impor a suspensão das atividades em razão da instabilidade ou da inviabilidade de acesso às plataformas eletrônicas.

O primeiro ataque virtual ocorreu no dia 3 de novembro de 2020 e atingiu o sistema eletrônico judicial do Superior Tribunal de Justiça, cujos dados ficaram inacessíveis a todos os usuários internos e externos do tribunal. Os criminosos criptografaram todos os dados aportados no sistema, inclusive os registrados em *backup*, exigindo pagamento de valores, em moeda virtual, para apresentação da chave de descriptografia[112]. Em comunicado oficial, o Superior Tribunal de Justiça informou que se tratou do "pior ataque cibernético já empreendido contra uma instituição pública brasileira, em termos de dimensão e complexidade", o que impôs a interrupção das atividades por quatro dias até o completo restabelecimento do acesso virtual.

No dia 11 de novembro de 2020 o Tribunal de Justiça do Rio Grande do Sul identificou um ataque cibernético ilegal ao sistema de processo eletrônico (eproc), em que o responsável, além de provocar a suspensão de acesso aos processos judiciais, deixou uma mensagem de ataque ao Judiciário, que permaneceu visível por mais de uma hora[113]. Em nota de esclarecimento, o Tribunal de Justiça do Rio Grande do Sul informou que o "*hotsite* informativo do eproc foi adulterado por *hackers*, porém sem comprometimento dos sistemas do Tribunal de Justiça"[114]. Ainda segundo o tribunal gaúcho, os processos e bancos de dados do judiciário estadual não foram atingidos, sendo certo que foi realizado um reforço de proteção para impedir novos acessos não autorizados.

Em 15 de novembro de 2020, o então Presidente do Tribunal Superior Eleitoral, Ministro Luís Roberto Barroso, confirmou o ataque cibernético aos sistemas eletrônicos computacionais do tribunal, sem que os criminosos lograssem êxito na captura de dados, a não ser o atraso na contabilização de votos das eleições municipais, ocorridas em 2020. Também no mês de novembro de 2020, no dia 27, o Tribunal Regional Federal da 1ª

---

[112] ALVES, Paulo. Ataque hacker ao STJ: seis coisas que você precisa saber sobre o caso. TechTudo, [*s. l.*], 7 nov. 2020. Disponível em: https://www.techtudo.com.br/listas/2020/11/ataque-hacker-ao-stj-seis-coisas-que-voce-precisa-saber-sobre-o-caso.ghtml. Acesso em: 16 jun. 2022.

[113] SISTEMA de processos do TJ-RS sofre ataque hacker nesta quarta-feira. Revista Consultor Jurídico, [s. l.], 11 nov. 2020. Disponível em: https://www.conjur.com.br/2020-nov-11/sistema-eproc-tj-rs-sofre-ataque-hacker-nesta-quarta-feira. Acesso em: 16 jun. 2022.

[114] RIO GRANDE DO SUL. Tribunal de Justiça do Estado do Rio Grande do Sul. Nota de esclarecimento. Porto Alegre: TJRS, 11 nov. 2020. Disponível em: https://www.tjrs.jus.br/novo/noticia/nota-de-esclarecimento-3/. Acesso em: 16 jun. 2022.

Região foi vítima de acesso virtual ilegal, causando a suspensão do acesso público ao site, que só veio a ser restabelecido três dias após o ataque, ainda assim, de forma gradual[115].

Na sequência dos ataques cibernéticos, no dia 15 de janeiro de 2021 o sistema eletrônico de processo do Tribunal Regional Federal da 3ª Região foi violado, sobrecarregando os sítios da corte, com instabilidade no sistema, até que a área de Tecnologia da Informação pudesse conter a agressão virtual e salvaguardar as informações processuais e o próprio sistema. Em nota oficial, o Tribunal Regional Federal da 3ª Região informou haver sofrido o "ataque cibernético do tipo DDOS, que sobrecarregou os sítios do Tribunal e provocou instabilidade ao longo do dia". A nota informou, ainda, que a área de tecnologia empreendeu esforços para conter o ataque, evitando a invasão às bases de dados processuais e administrativas tratadas pelo respectivo Tribunal.

Não obstante o prometido reforço de proteção para obstar novos ataques cibernéticos, no dia 28 de abril de 2021 o Tribunal de Justiça do Estado do Rio Grande do Sul foi vítima de novo ataque virtual, dessa vez com atuação exitosa de criminosos, que corromperam todo o sistema operacional, sinalizando a cobrança de valores, em criptomoedas, para fornecer as chaves que poderiam decodificar o conteúdo criptografado em servidores e estações de trabalho[116].

No dia 6 de maio de 2021, os ataques aos sistemas eletrônicos do Judiciário brasileiro foram dirigidos ao Supremo Tribunal Federal, sobrevindo a declaração de que a violação atingiu somente usuários externos. Segundo informação, a invasão virtual foi contida enquanto ainda estava em andamento, e "não foram acessadas informações sigilosas nem houve sequestro do ambiente virtual"[117]. Em Agosto de 2022, o Tribunal de Justiça do Distrito Federal e Territórios – TJDFT também sofreu tentativa de acesso por *hackers* ao banco de dados da Corte, permanecendo o PJE fora do ar por vários dias. Em nota, o TJDFT informou que "foi detectada atividade maliciosa" e que "o incidente está em apuração interna e também pela Polícia Civil, com prioridade para o

---

[115] ORTIZ, Brenda. Por suspeita de ataque hacker, TRF-1 retira do ar portal da Justiça Federal do DF e de 13 estados. *G1*, Brasília, 27 nov. 2020. Disponível em: https://g1.globo.com/df/distrito-federal/noticia/2020/11/27/por-suspeita-de-ataque-hacker-trf-1-retira-do-ar-portal-da-justica-federal-do-df-e-de-13-estados.ghtml. Acesso em: 16 jun. 2022.

[116] POLÍCIA Civil inicia investigação sobre ataque cibernético ao sistema do TJ-RS. G1, [*s. l.*], 30 abr. 2021. Disponível em: https://g1.globo.com/rs/rio-grande-do-sul/noticia/2021/04/30/policia-civil-inicia-investigacao-sobre-ataque-ao-sistema-informatico-do-tj-rs.ghtml. Acesso em: 16 jun. 2022.

[117] FALCÃO, Márcio; VIVAS, Fernanda. Supremo investiga suposto ataque hacker a sistema da Corte. G1, Brasília, 7 maio 2021. Disponível em: https://g1.globo.com/politica/noticia/2021/05/07/supremo-investiga-tentativa-de-ataque-hacker-a-sistema-da-corte.ghtml. Acesso em: 16 jun. 2022.

restabelecimento dos sistemas judiciais". A Corte esclareceu, ainda, que "não houve interrupção da jurisdição, que continua a ser prestada pelos desembargadores e juízes, em regime de plantão permanente"[118].

Diante dos ataques sofridos pelo Judiciário relatados acima é possível afirmar que não houve nenhum esclarecimento aos cidadãos sobre o real alcance da violação ou o grau de comprometimento das informações processuais públicas ou sigilosas, indevidamente acessadas. Não houve informação sobre a titularidade dos dados e quais os dados sequestrados. Não se demonstrou a adoção de medidas eficazes que comprovassem o cumprimento das normas de proteção de dados. Não houve transparência sobre a forma de tratamento de dados, sobre as medidas técnicas e administrativas empregadas na solução do problema, ou ainda, sobre as medidas preventivas para sustar os danos decorrentes do vazamento, todas condições erigidas no art. 6º da Lei nº 13.709/2018, como princípios a serem observados.

A despeito de medidas de segurança e prevenção, os sistemas eletrônicos de gestão processual não só foram acessados de forma ilegal, como dados e informações pessoais e empresariais sigilosos, íntimos e privados, confiadas ao Estado, foram recolhidas de forma não consentida e possivelmente tratados para outros fins. O êxito na conversão do processo judicial físico em eletrônico, aliado à certeza de que o sistema operacional eletrônico fosse seguro o bastante para guarda de informações processuais, diretamente relacionadas às partes litigantes identificadas, impuseram aos tribunais o agir corretivo, consequencial, não obstante o dano consumado. A partir do êxito na conquista do mundo digitalizado, o homem passou a viver as consequências do agir tecnológico, experimentando a transformação que lhe foi imposta por esse agir, sem medir os efeitos diretos e indiretos, cegos pelo otimismo que sua imaginação poderia ou deveria ter antevisto[119].

O poder tecnológico é absoluto até a próxima inovação. A segurança do sistema operacional computadorizado é absoluta até a ocorrência do próximo episódio, que demonstre sua fragilidade e imponha a remediação do dano, como se a dignidade, a individualidade e autenticidade humana, asseguradas pela privacidade e liberdade,

---

[118] METRÓPOLES. Após ataque hacker, site do TJDFT segue fora do ar pelo 3º dia seguido. Disponível em: https://www.metropoles.com/distrito-federal/apos-ataque-hacker-site-do-tjdft-segue-fora-do-ar-pelo-3o-dia-seguido. Acesso em: 21 nov. 2022.

[119] PELLEGRINO, Maria Cristina Conde. *DA MIHI DATA, DABO TIBI JUS*: o tratamento de dados pessoais no âmbito do processo judicial eletrônico brasileiro, à luz da Lei Geral de Proteção de Dados' 13/07/2021 147 f. Dissertação (Mestrado em Instituições Sociais, Direito e Democracia) - Universidade FUMEC, Belo Horizonte Biblioteca Depositária: FCH, 2021.

pudessem ser reparados ou compensados, pela próxima criação tecnológica[120]. Dito isso, é possível afirmar que a frequência em pouco tempo de ataques maliciosos no Judiciário mostra que o sistema de segurança e prevenção adotados pelos Tribunais ainda são muito frágeis e vulneráveis, motivo que os tornam alvos de ataques, invasões e atividades maliciosas. Acredita-se que as melhores soluções para evitar essas invasões seria, tanto a LGPD, como as resoluções normativas do CNJ criadas para melhor adequar os Tribunais à lei, estipularem a adoção padronizada de certos sistemas de segurança e prevenção mais avançados, diferente da realidade de hoje, onde cada tribunal tem autonomia para escolher quais sistemas e medidas de segurança devem ser adotados para proteger os dados coletados e armazenados por eles.

Para isso, se faz necessário um melhor investimento pelos Tribunais em equipes de TI e segurança bem capacitadas, assim como em tecnologias mais avançadas, como forma de melhorar a proteção de seus sistemas. Porém, para que isso se concretize, se faz necessária a fiscalização com mais frequência da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e de demais órgãos fiscalizatórios com o intuito de dar mais efetividade à norma, o que será visto no próximo capítulo.

3.6 DO COMPARTILHAMENTO DE DADOS PELO PODER PÚBLICO

O compartilhamento de dados pessoais é a operação de tratamento pela qual órgãos e entidades públicas conferem permissão de acesso ou transferem uma base de dados pessoais a outro ente público ou a entidades privadas visando ao atendimento de uma finalidade pública. De forma mais específica, a LGPD utiliza o termo “uso compartilhado de dados”, que é definido como a:

> comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

[120] PELLEGRINO, Maria Cristina Conde. *DA MIHI DATA, DABO TIBI JUS*: o tratamento de dados pessoais no âmbito do processo judicial eletrônico brasileiro, à luz da Lei Geral de Proteção de Dados' 13/07/2021 147 f. Dissertação (Mestrado em Instituições Sociais, Direito e Democracia) - Universidade FUMEC, Belo Horizonte Biblioteca Depositária: FCH, 2021.

Os órgãos do Poder Judiciário possuem uma das maiores bases de dados em relação aos demais órgãos da Administração Pública, cuja base de dados que poderá ser compartilhada, se não acompanhada de salvaguardas efetivas aos direitos dos indivíduos, é deveras preocupante, de maneira que é preciso que se reflita acerca do controle dos dados relativos à personalidade do indivíduo (sexo, escolaridade, residência, data de nascimento, filiação, entre outros). O compartilhamento de informações facilita o acesso a detalhes privados da vida dos cidadãos. Ainda mais na sociedade atual, permeada por dispositivos informáticos que permitem o processamento de milhares de informações a partir de apenas um click e possibilita que a informação circule ao redor do mundo com celeridade impressionante[121].

Quando um indivíduo fornece dados a uma determinada repartição pública ou é pessoalmente associado a informações, ele o faz para um determinado propósito, quase sempre vinculado a área de atuação daquela entidade. Ao quebrar as barreiras entre os diferentes órgãos e entidades do Estado e permitir o compartilhamento, dados podem ganhar novo propósito para além do que foram coletados inicialmente. Exemplo típico é o acordo de cooperação firmado entre o Tribunal Superior Eleitoral e o SERASA S/A, no qual dados sensíveis dos eleitores seriam repassados à empresa citada podendo causar desvio de finalidades com os dados obtidos[122].

Entretanto, o uso compartilhado de dados pela Administração Pública pressupõe a "capacidade de diversos sistemas e organizações trabalharem em conjunto, de modo a garantir que pessoas, organizações e sistemas computacionais troquem dados", ou seja, a chamada interoperabilidade desses diversos sistemas e bancos de dados. Tal previsão já constava do artigo 24, III e IV do Marco Civil da Internet (Lei nº 12.965/2014).

O Poder Judiciário e órgãos integrantes do sistema de justiça, a exemplo da AGU (Termo de Acordo e Cooperação Técnica nº 058/2009) e Ministério Público (Resolução Conjunta nº 03/2013), adotaram o Modelo Nacional de Interoperabilidade – MNI, com vistas a adoção de um padrão nacional de sistemas de processo eletrônico utilizando a tecnologia "WebService" (cláusula primeira do Termo de Acordo e Cooperação Técnica nº 058/2009), integrando a base de dados de informações processuais entre as instituições,

---

[121] LIMA, Jose Jeronimo Nogueira de. *LGPD e administração pública*: regulação e aplicação' 26/01/2021 147 f. Dissertação (Mestrado em Direito) - Pontifícia Universidade Católica de São Paulo, São Paulo Biblioteca Depositária: PUC/SP, 2021.

[122] LIMA, Jose Jeronimo Nogueira de. *LGPD e administração pública*: regulação e aplicação' 26/01/2021 147 f. Dissertação (Mestrado em Direito) - Pontifícia Universidade Católica de São Paulo, São Paulo Biblioteca Depositária: PUC/SP, 2021.

viabilizando, por exemplo, dentro dos órgãos do Poder Judiciário que um recurso originário do Tribunal Regional Federal da 1ª Região seja encaminhado ao Superior Tribunal de Justiça pelo próprio sistema. Esse modelo, criado pelo CNJ, tem, para além da finalidade de interoperar os diversos sistemas do judiciário, "a função primordial de interligar o sistema do poder judiciário com sistemas externos"[123].

Avaliar se esse sistema e os demais utilizados pelo Judiciário estão sendo utilizados conforme as normas da LGPD, sem fugir das finalidades propostas, é uma boa pesquisa a se fazer no futuro em um próximo trabalho. Porém, o foco do presente estudo é apresentar a parte normativa da lei para que o Poder Público possa seguir suas regras de compartilhamento de dados de forma eficiente, sempre priorizando a proteção dos dados pessoais. Desse modo, o artigo 25 da LGPD prevê que os dados deverão ser mantidos em formato interoperável e estruturado para seu uso compartilhado, com vistas "à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral".

Conforme se depreende do artigo 7º, III da LGPD, não é necessário o consentimento do titular de dados pessoais para o compartilhamento de dados pessoais entre órgãos e entidades do Poder Público. O uso compartilhado de dados entre órgãos e entidades públicas pressupõe, logicamente, que tal operação é realizada para "o cumprimento de suas competências legais", nos limites do conceito de compartilhamento previsto no art. 5º da LGPD, conjugado com o previsto no artigo 25 da lei, que delimita esta competência à execução de políticas públicas, prestação de serviços, descentralização da atividade pública e disseminação de informações ao público.

Porém, isso não faz com que o Poder Público não tenha que dar nenhuma informação ao titular do dado. Pelo contrário, os atos que regem e autorizam o compartilhamento de dados pessoais devem prever as formas de atendimento ao princípio da transparência (art. 6º, VI), assegurando a disponibilização de informações claras, precisas e facilmente acessíveis aos titulares sobre a realização do compartilhamento e sobre como exercer seus direitos. Constitui uma boa prática divulgar na página eletrônica

---

[123] LIMA, Jose Jeronimo Nogueira de. *LGPD e administração pública*: regulação e aplicação' 26/01/2021 147 f. Dissertação (Mestrado em Direito) - Pontifícia Universidade Católica de São Paulo, São Paulo Biblioteca Depositária: PUC/SP, 2021.

dos órgãos e das entidades responsáveis as informações pertinentes nos termos do art. 23, I, da LGPD.

Também é importante que sejam estabelecidas as medidas de segurança, técnicas e administrativas, que serão adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (art. 6º, VII, e 46, da LGPD). Essas medidas, que devem ser proporcionais aos riscos às liberdades civis e aos direitos fundamentais dos cidadãos envolvidos no caso concreto, deverão estar previstas nos atos que regem e autorizam o compartilhamento dos dados. Já o artigo 26 da LGPD prevê que o compartilhamento de dados deve respeitar os princípios da proteção de dados previsto no artigo 6º da lei, com destaque aos princípios da finalidade e necessidade, de tal forma que esteja adstrito a finalidade que o determinou e seja restrito ao mínimo necessário para realização desse fim.

O artigo 30 da LGPD, por sua vez, consigna que a ANPD "poderá estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais". Inclusive, é previsto um capítulo específico (VII) acerca da segurança e boas práticas relacionadas à proteção de dados, atribuindo, tanto à ANPD (art. 46, §1º), quanto aos agentes de tratamento de dados (art. 50, §1º), dispor de padrões técnicos para a realização de regras de governança de dados, o que abrange políticas para o compartilhamento.

Já o art. 37 da LGPD prevê que o uso compartilhado de dados pessoais deve ser formalizado, com obrigatoriedade de realização de registro das operações de tratamento. Para tanto, recomenda-se a instauração de processo administrativo, do qual constem os documentos e as informações pertinentes, incluindo análise técnica e jurídica, conforme o caso, que exponham a motivação para a realização do compartilhamento e a sua aderência à legislação em vigor. Além disso, recomenda-se que o compartilhamento seja estabelecido em ato formal, a exemplo de contratos, convênios ou instrumentos congêneres firmados entre as partes. Outra possibilidade é a expedição de decisão administrativa pela autoridade competente, que autorize o acesso aos dados e estabeleça os requisitos definidos como condição para o compartilhamento.

Já em relação ao tempo de duração do compartilhamento, o tratamento de dados pessoais é um processo com duração definida, após o qual, em regra, os dados pessoais devem ser eliminados, observadas as condições e os prazos previstos em normas específicas que regem a gestão de documentos e arquivos. Vale ressaltar que o art. 16 da

LGPD estabelece hipóteses gerais em que é autorizada a conservação de dados pessoais. Logo, a delimitação do período de duração do uso compartilhado dos dados também é relevante para o fim de reavaliação periódica do instrumento que autorizou o compartilhamento, incluindo a possibilidade de sua adequação a novas disposições legais e regulamentares ou a previsão de novas medidas de segurança, de acordo com as tecnologias disponíveis.

Por sua vez, nos casos de uso compartilhado de dados pessoais entre entes públicos e entidades privadas, é necessário observar os requisitos adicionais e específicos indicados no art. 26, § 1º e no art. 27 da LGPD. Em especial, deve-se considerar que eventual transferência de dados pessoais para entidades privadas somente será admitida se amparada em uma das seguintes hipóteses: (i) nos casos de execução descentralizada da atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado; (ii) nos casos de dados acessíveis publicamente; (iii) quando houver previsão legal ou a transferência for respaldada em contratos e instrumentos congêneres; ou (iv) na hipótese de a transferência objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades.

Por fim, em muitos casos pode ser necessário identificar as funções e responsabilidades dos agentes de tratamento envolvidos no uso compartilhado de dados pessoais. Em caso de compartilhamento de dados entre controlador e operador, por exemplo, podem ser detalhadas as instruções e as condições que devem ser observadas pelo operador ao realizar o tratamento dos dados pessoais, conforme art. 39 da LGPD.

Diante do exposto, é possível afirmar que o uso compartilhado de dados pessoais deve ser realizado em conformidade com a LGPD, notadamente com os princípios previstos no art. 6º, as bases legais previstas nos arts. 7º ou 11 (em casos de dados pessoais sensíveis), garantia dos direitos dos titulares e outras regras específicas aplicáveis ao Poder Público. Além de conferir maior previsibilidade, transparência e segurança jurídica ao uso compartilhado de dados, a observância dessas disposições legais constitui peça-chave para a promoção de uma relação de confiança com os titulares e para a adequada gestão de riscos pelos controladores, inclusive para evitar a ocorrência de abusos e desvios de finalidades.

Em verdade, a proteção de dados pessoais deveria se apresentar como um limite ao compartilhamento, especialmente quando fragiliza o exercício de outros tantos direitos correlatos à privacidade. Ter o compartilhamento de dados como regra é uma lógica que

aniquila o poder da autodeterminação enquanto direito principiológico basilar da disciplina da proteção de dados. Como já visto, o cidadão é muitas vezes obrigado a informar dados pessoais para o Poder Judiciário com o intuito de alcançar a prestação jurisdicional, sem grande debate acerca da base legal. Infelizmente, essa ainda é nossa embrionária cultura de governança. Quando esses dados são automaticamente compartilhados com outros órgãos públicos, maximiza-se ainda mais a restrição à sua autodeterminação. Portanto, o fato de os nossos dados serem sediados por órgãos públicos não os faz públicos. Eles seguem sendo pessoais. Nesse cenário, destaca-se a importância da jurisdição na contenção de violações, o que será apresentado no capítulo a seguir.

4 PERSPECTIVAS DO TRATAMENTO DE DADOS PESSOAIS PELO PODER JUDICIÁRIO À LUZ DA LGPD

No primeiro capítulo deste trabalho foi apresentada uma visão histórica da evolução da proteção de dados pessoais no ordenamento jurídico de alguns países da União Europeia, que foram exemplos de modelos para o ordenamento jurídico de outros países, principalmente do Brasil, assim como a evolução da proteção de dados dentro do ordenamento jurídico brasileiro até a chegada da lei principal que trata sobre o tema, a Lei Geral de Proteção de Dados Pessoais. Após, foram apresentados conceitos da referida lei e do tratamento de dados pelo Poder Público que serviram como base para a exposição dos capítulos seguintes. Já no segundo capítulo foram apresentados alguns dos principais problemas e desafios enfrentados pelo Poder Judiciário brasileiro na adequação às normas da LGPD, para, por fim, chegar ao último capítulo deste trabalho e propor perspectivas de tratamento de dados pessoais ao Judiciário à luz da LGPD para mais efetividade da lei e na proteção dos direitos fundamentais da privacidade, intimidade e proteção de dados pessoais.

4.1 DAS PRERROGATIVAS E OBRIGAÇÕES

A LGPD fez questão de incluir prerrogativas indispensáveis no tratamento de dados pelo Poder Público por possuir uma grande coleta e armazenamento de dados pessoais, zelando pela proteção dos dados pessoais e pela garantia dos direitos da personalidade humana, sendo possível a isenção da fiscalização, sob a premissa de interesse público. Mesmo visando o interesse geral, o Poder Público não pode prescindir dos princípios, fundamentos e objetivos que norteiam a tutela da proteção de dados no Brasil, tais como o princípio da finalidade, da adequação, da transparência, da segurança, da prevenção e da responsabilização e prestação de contas, explicitados no art. 6º da LGPD.

Partindo para as prerrogativas do Poder Público, onde é possível citar o judiciário, a partir da Lei nº 13.709, de 2018, o tratamento de dados pessoais dependerá, necessariamente, de que o titular de dados seja informado de forma clara e atualizada, preferencialmente no sítio eletrônico próprio, sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, mesmo que o consentimento para tratamento de dados seja dispensável. Dependerá, ainda, da indicação

de um encarregado pela operação de tratamento de dados, que deverá observar as instruções do controlador dos dados, que, por sua vez, será o interlocutor com o titular dos dados.

Outra prerrogativa trazida pela LGPD que deverá ser aplicada pelo Judiciário é o acesso estruturado e compartilhado de dados formatados por outras pessoas de direito público que, por meio de uma dinâmica interoperável, podem se valer de informações pessoais, sensíveis ou não, para execução de políticas públicas, estabelecidas em nome do interesse público, na forma autorizada pelos artigos 25, 26 e 27 da Lei nº 13.709, de 2018, sem, contudo, nunca prescindir da observância dos princípios de proteção de dados pessoais, elencados no art. 6º da LGPD.

Nesse sentido, o Judiciário enquanto submetido ao regramento de proteção de dados, qualquer ato que importe em tratamento de dados pessoais, na forma definida pela LGPD, impõe além da observância de todos os princípios elencados no art. 6º da Lei nº 13709 de 2018, a transparência na persecução do interesse público, na execução de competências legais, com a necessária informação da base legal autorizadora do tratamento de dados prevista nos arts. 7º e 11º da LGPD, conforme já abordados no primeiro capítulo deste trabalho. Entre os princípios que norteiam a atividade de tratamento de dados, sobreleva o princípio da transparência, da segurança, da prevenção e da responsabilização e prestação de contas, expressos nos incisos VI, VII, VIII e X, todos do art. 6º da LGPD.

Pelo princípio da transparência é garantido aos titulares de dados pessoais informações claras, precisas e facilmente acessíveis sobre a realização do tratamento de dados e sobre os agentes encarregados, “observados os segredos comercial ou industrial”. A observação que excetua a garantia de informação não importa na ocultação do aviso de tratamento, mas sim na preservação do método de tratamento, se envolver tecnologia comercial.

O princípio da segurança considera o uso de medidas técnicas e administrativas hábeis a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas que podem levar a destruição, perda, alteração, comunicação ou difusão não autorizadas. Juntamente com o princípio da prevenção, que impõe medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais, em especial, para evitar a circulação não autorizada de informações pessoais, o princípio da segurança se apresenta como uma das obrigações essenciais e primordiais para proteção dos “direitos

fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade natural", indicados como objeto da LGPD.

Dito isso, conforme visto os ataques frequentes de *hackers* e vazamento de dados pessoais nos sistemas do Judiciário no capítulo anterior, se faz necessário o investimento pelos tribunais em práticas de proteção de dados eficientes e atualizadas que façam frente às ameaças externas, antecipando-se aos cenários de quebra de segurança, que importem no acesso e no manuseio indevido dos dados das pessoas naturais, objeto do tratamento. A segurança que se espera não é aplicada exatamente aos dados em si, mas sim aos sistemas que os mantém (medidas técnicas) e ao ambiente geral da instituição (medidas organizativas). Isso significa que não bastam as medidas técnicas, como o uso de firewall, métodos criptografados e controles de conteúdo, se elas não vieram acompanhadas de outras medidas, como treinamento de segurança, criação de políticas de segurança da informação, inventários de ativos etc.[124]

O desconhecimento da tecnologia não pode ser erigido como escusa para violação a direitos fundamentais, quando, por mais "exógena que possa parecer, a tecnologia é um produto do homem e de sua cultura, destinada a relacionar-se com ele"[125]. Por meio da técnica digital o homem se reorganizou para operar e influir na sociedade, de modo a propor uma readaptação dos institutos a essa realidade, considerando o saber fazer e a responsabilidade sobre seus atos. Desse saber fazer e da responsabilidade sobre seus atos exsurge o princípio da responsabilidade e da prestação de contas no tratamento de dados pessoais, que requer do agente a efetiva prática de procedimentos de segurança, com observância aos objetivos, fundamentos e princípios da LGPD, num verdadeiro programa de *compliance*.

Para responder pelo princípio da responsabilidade e da prestação de contas, há que se considerar cumpridos os princípios da segurança e da prevenção, para, então, o agente controlador de dados pessoais vir a ser cobrado em sua responsabilidade de utilizar os procedimentos necessários, viáveis e disponíveis, demonstrando, ainda, que as providências eleitas surtiram a eficácia esperada, não bastando a mera boa-fé no tratamento de dados.

---

[124] MENKE, Fabiano; GOULART, Guilherme Damasio. Segurança da Informação e Vazamento de Dados. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (coord.). Tratado de Proteção de Dados. Rio de Janeiro: Forense, 2021. p. 346.

[125] DONEDA, Danilo. Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019, pg. 51.

Logo, os princípios da prevenção, da segurança e da responsabilidade são princípios que devem ser aplicados pelo judiciário como condição ao tratamento de dados, de modo a impor uma atuação preventiva incessante como única forma de fixar a noção de proteção de dados. Para tanto, é importante adotar medidas de segurança, técnicas e administrativas aptas à proteção de dados, de modo a evitar o acesso não autorizado, a destruição acidental ou ilícita do dado ou qualquer tratamento inadequado, bem como a adoção de boas práticas e governança, que estabeleçam as condições de organização, normas de segurança, padrões técnicos para mitigação de riscos.

Diante dessas obrigações e visando a melhor governança de dados pessoais o Governo Federal brasileiro publicou o "Guia de boas práticas: Lei Geral de Proteção de Dados (LGPD)"[126] no âmbito da Administração Pública, trazendo orientações sobre as bases legais e metodologia para o tratamento de dados, bem como para produção de relatório de impactos, ciclo de vida do tratamento de dados pessoais e padrões de segurança de informação. O guia para melhor governança deixa certo não bastar o enquadramento do tratamento de dados a uma das hipóteses legais autorizativas do arts. 7º e 11º, da LGPD. É imperioso garantir todos os princípios listados em lei, entre eles o princípio da prevenção e segurança, merecendo destaque a seguinte orientação:

> Segurança e proteção de ponta a ponta durante o ciclo de vida de tratamento dos Dados. Por ser incorporado ao sistema antes de o primeiro elemento de informação ser coletado, a PdC estende-se por todo o ciclo de tratamento dos dados envolvidos no projeto, sistema ou serviço. Medidas fortes de segurança são essenciais para a privacidade, do início ao fim. A privacidade deve ser protegida continuamente em todo o domínio e ao longo do ciclo de vida do tratamento dos dados em questão. Não deve haver lacunas na proteção ou na prestação de contas. O princípio "Segurança" tem relevância especial porque, em sua essência, sem segurança forte, não pode haver privacidade. As instituições devem assumir a responsabilidade pela segurança dos dados pessoais, geralmente proporcional ao grau de sensibilidade, durante todo o ciclo de tratamento, consistente com os padrões que foram definidos por organismos reconhecidos de desenvolvimento de padrões. Os padrões de segurança aplicados devem garantir a confidencialidade, integridade e disponibilidade dos dados pessoais durante todo o seu ciclo de tratamento, incluindo, entre outros, métodos de destruição segura, criptografia apropriada, e métodos fortes de controle de acesso e registro. Na LGPD, a segurança é um princípio a ser observado no tratamento de dados pessoais, destacado pelo art. 6º, inciso VII. Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de

[126] BRASIL. *Guia de boas práticas*: Lei Geral de Proteção de Dados (LGPD). Brasília, DF: Comitê Central de Governança de Dados, 2021. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf. Acesso em: 16 jun. 2022.

> acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão[127].

Com efeito, as regras principiológicas apresentadas nos incisos VI, VII, VIII e X do art. 6º da LGPD hão de ser observados pelos órgãos do judiciário, sob pena de violação aos seus preceitos básicos, além da desconsideração a princípios fundamentais, inerentes à dignidade da pessoa humana. Para o tratamento de dados no exercício da função jurisdicional não basta observar a finalidade, a adequação, a necessidade, o livre acesso, a qualidade e a não discriminação sobre os dados pessoais. Compete ao Judiciário, igualmente, observar todos os preceitos que importem no adequado tratamento dos dados pessoais, durante todo o procedimento judicial em que informações são coletados voluntária e involuntariamente, em razão da confiança, da boa-fé e da expectativa da não surpresa, na certeza de que os dados pessoais dos jurisdicionados não serão utilizados para qualquer outro fim, por qualquer pessoa que tenha acesso às referidas informações, senão para o julgamento judicial. Impõe-se a conduta fundada em boas práticas e governança eficaz, adotando, para isso, todas as medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais que, em última análise, correspondem à expressão da personalidade humana, e por isso à dignidade da pessoa humana[128].

Não existem dados inúteis. Qualquer informação pessoal é uma projeção da personalidade e qualquer tratamento de dados, legitimado ou não, pode influenciar a representação da pessoa na sociedade, com potencial de violar direitos fundamentais. Adequar-se e responder pelas novas demandas sociais são os principais objetivos do Poder Público na elaboração, na execução ou na aplicação das leis. Ao coletar, transmitir, publicar e arquivar dados pessoais o Poder Público submete-se a LGPD, e na sua atividade jurisdicional deverá ser igualmente responsivo às regras legais, demonstrando a eficácia de medidas, em prol da efetividade da proteção de dados pessoais.

4.2 DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS – ANPD E RESPONSABILIDADE CIVIL DO PODER PÚBLICO

---

[127] BRASIL. *Guia de boas práticas*: Lei Geral de Proteção de Dados (LGPD). Brasília, DF: Comitê Central de Governança de Dados, 2021.

[128] PELLEGRINO, Maria Cristina Conde. *DA MIHI DATA, DABO TIBI JUS*: o tratamento de dados pessoais no âmbito do processo judicial eletrônico brasileiro, à luz da Lei Geral de Proteção de Dados' 13/07/2021 147 f. Dissertação (Mestrado em Instituições Sociais, Direito e Democracia) - UNIVERSIDADE FUMEC, Belo Horizonte Biblioteca Depositária: FCH, 2021.

Não adianta falar de prerrogativas, obrigações, princípios a serem seguidos pelo Poder Público, no caso, o Poder Judiciário, se não tiver um ou mais órgãos fiscalizadores de tudo isso. Assim, a LGPD trouxe a Autoridade Nacional de Proteção de Dados Pessoais (ANPD) para cumprir esse papel. Porém, é necessário fazer uma análise se as funções e medidas fiscalizadoras trazidas pela LGPD à ANDP, no que se refere ao Poder Público, estão sendo efetivas à proteção de dados pessoais.

O Governo Federal emitiu um guia de boas práticas de Tratamento de Dados pelo Poder Público[129] e conceituou a ANPD como sendo o órgão central de interpretação da LGPD e do estabelecimento de normas e diretrizes para sua implementação, no que se inclui a deliberação administrativa, em caráter terminativo, sobre a interpretação da lei e sobre as suas próprias competências e casos omissos (art. 55-K, parágrafo único; art. 55-J, XX). Além disso, a autoridade nacional detém competência exclusiva para aplicar as sanções administrativas previstas na LGPD, com prevalência de suas competências sobre outras correlatas de entidades e órgãos da administração pública no que se refere à proteção de dados pessoais (art. 55-K).

Assim, o guia complementa que a ANPD possui competência originária, específica e uniformizadora no que concerne à proteção de dados pessoais e à aplicação da LGPD, previsão legal que deve ser interpretada de forma a se compatibilizar com a atuação de outros entes públicos que possam eventualmente tratar sobre o tema. A esse respeito, a LGPD (art. 55-J, § 3º) estabelece que a ANPD deve atuar em coordenação e articulação com outros órgãos e entidades públicas, visando assegurar o cumprimento de suas atribuições com maior eficiência e promover o adequado funcionamento dos setores regulados[130].

Contudo, existe uma polêmica em relação às referidas disposições normativas que dizem respeito à atuação da ANPD perante os órgãos e entidades do Poder Público, à luz do pacto federativo e da repartição de Poderes. Nos termos do art. 55-A da LGPD, a ANPD é órgão da administração pública federal, integrante da Presidência da República. Em até 2 anos da entrada em vigor da estrutura regimental da ANPD, a Autoridade poderá ser transformada em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada – porém não subordinada – à Presidência da

[129] BRASIL. Guia de boas práticas: Lei Geral de Proteção de Dados (LGPD). Brasília, DF: Comitê Central de Governança de Dados, 2021. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf. Acesso em: 16 jun. 2022.
[130] Conforme o Parecer n° 00018/2021/GAB/ASJUR-ANPD/CGU/AGU (NUP 0130.000035/2021-97) sobre a abrangência da competência da ANPD.

República (o que é fortemente recomendado pela doutrina para assegurar a independência e a autonomia necessárias à atuação da ANPD)[131]. Estudo realizado pelo Instituto Brasileiro de Defesa do Consumidor (IDEC) sobre os modelos das autoridades de proteção de dados na América Latina apontou preocupações quanto à subordinação dessas entidades às Presidências de diversos países, como atualmente ocorre no modelo brasileiro – considerada um fator de risco à autonomia da autoridade.

O fato de a ANPD ser órgão da administração pública federal direta levanta dúvidas sobre a possibilidade de imposição de medidas a outros órgãos e entidades do Poder Público, outros entes federativos ou até mesmo outros Poderes, especialmente quando suas determinações gerarem despesas a tais agentes de tratamento de dados (como parece ser o caso da solicitação de informações do art. 29; das medidas referidas pelo art. 31; e da elaboração dos relatórios de impacto referidos no art. 32).

Diante desse questionamento, Fernando Antônio Tasso ponderou que tais disposições normativas não outorgariam poder requisitório à ANPD em face de outros órgãos integrantes do Poder Público (ou seja, as medidas da ANPD teriam um caráter de recomendação)[132]. Entretanto, reconhecer que a ANPD não pode efetivamente impor medidas a esses destinatários certamente enfraquece a Autoridade diante de agentes cujo risco de violação da LGPD é extremamente relevante[133].

Assim, entende-se que a transformação da ANPD em autarquia especial na forma e no prazo previstos na LGPD – passando a ser dotada de independência administrativa, ausência de subordinação hierárquica, mandato fixo e estabilidade de seus dirigentes e autonomia financeira – é movimento necessário não apenas para outorgar à Autoridade os poderes e recursos para que cumpra de forma adequada com suas funções legais, mas também para evitar questionamentos de ordem hierárquica e federativa quando o agente de tratamento de dados em questão integrar o Poder Público.

Porém, tal questão foi suprida pelo atual governo. Foram com esses entendimentos que foi criada, pelo Presidente da República, Jair Messias Bolsonaro, a Medida Provisória nº 1.124/22, já aprovada pela Câmara dos Deputados e o Senado Federal, em 18 de outubro de 2022, a qual transforma a Autoridade Nacional de Proteção de Dados (ANPD)

---

[131] Nesse sentido, cf. OLIVEIRA, Caio César de. A Autoridade Nacional de Proteção de Dados (ANPD) e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. *In*: MULHOLLAND, Caitlin (coord.). *A LGPD e o novo marco normativo do Brasil*. Porto Alegre: Arquipélago, 2020. p. 380-383; e TERRA; CASTRO, op. cit., p. 254-255.
[132] TASSO, 2019, p. 286.
[133] OLIVEIRA, 2020, p. 389.

em autarquia especial, ou seja, não mais subordinada à Presidência da República, passando a ter uma gestão administrativa e financeira descentralizada e autônoma[134]. Essa medida provisória foi um grande avanço para a maior efetividade da fiscalização pela Autarquia. Portanto, suprida a questão acima, necessário se faz a análise das funções que poderão ser exercidas pela ANPD ao Poder Público à luz da LGPD.

Especificamente em relação ao Poder Público, a LGPD (art. 55-J, XI e XVI) prevê que a ANPD pode solicitar informe específico sobre o âmbito, a natureza dos dados e demais detalhes envolvidos na operação, bem como realizar auditorias sobre o tratamento de dados pessoais. Já o art. 52, § 3°[135], estabelece quais sanções podem ser aplicadas às entidades e aos órgãos públicos, com expressa exclusão das penalidades de multa simples ou diária previstas na LGPD. Em relação às penalidades aplicadas, uma grande diferença da aplicação da LGPD aos órgãos públicos para o âmbito privado é que, para a Administração Pública, não há a previsão de sanção pecuniária, mas apenas a advertência, a publicização da infração, bloqueio ou eliminação dos dados pessoais a que se refere a infração, sem prejuízo das sanções previstas no Estatuto do Servidor Público Federal, na lei de Improbidade Administrativa e na lei de acesso à informação.

A impossibilidade de imposição de multa ao Estado se justifica pelo próprio senso de coletividade de não onerar o contribuinte em razão das falhas do Estado (a Administração Pública é sustentada pelos cidadãos através do recolhimento de impostos).

---

[134] TECMASTERS. Senado aprova MP que dá autonomia à Autoridade de Proteção de Dados. Disponível em: https://tecmasters.com.br/senado-mp-autonomia-autoridade-protecao-dados/. Acessado em: 11. dez 2022.

[135] Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
I - advertência, com indicação de prazo para adoção de medidas corretivas;
II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
III - multa diária, observado o limite total a que se refere o inciso II;
IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
VI - eliminação dos dados pessoais a que se refere a infração;
VII - (VETADO);
VIII - (VETADO);
IX - (VETADO).
X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.
§ 3º O disposto nos incisos I, IV, V, VI, X, XI e XII do **caput** deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990, na Lei nº 8.429, de 2 de junho de 1992, e na Lei nº 12.527, de 18 de novembro de 2011.

Porém, a falta de punição efetiva e sancionadora pode servir como estímulo para o não cumprimento da norma pelo Poder Público, motivo em que a ANPD, mesmo sendo um órgão da Administração Pública, precisará punir de forma efetiva o Poder Público quando da violação à proteção de dados pessoais, a fim de dar efetividade à norma.

Entretanto, mesmo que não haja previsão de sanção pecuniária ao Poder Público, o servidor público que infrinja a LGPD é passível de responsabilização administrativa pessoal e autônoma, conforme o art. 28 do Decreto Lei n° 4.657, de 4 de setembro de 1942 (Lei de Introdução às normas do Direito Brasileiro), Lei nº 8.112/1990 (Estatuto do Servidor Público Federal), da Lei nº 8.429/1992 (Lei de Improbidade Administrativa) e da Lei nº 12.527/2011 (Lei de Acesso à Informação)"[136]. Dessa forma, tratar dados pessoais indevidamente, como por exemplo vendendo banco de dados, alterando ou suprimindo cadastros de forma inadequada ou usando dados pessoais para fins ilegítimos, pode levar à responsabilização do servidor público que praticou o ato ilegal. Por outro lado, no âmbito da responsabilidade civil do Poder Público, a LGPD não apresentou disposições especificas. Por isso, ao se tratar do tema deverá ser aplicada a regra geral prevista na LGPD e as demais normas já existentes no ordenamento jurídico, aplicando o diálogo das fontes.

Dentre as regras gerais, o artigo 2º da LGPD prevê como um dos 10 princípios nele elencados o princípio da responsabilização, no qual "os agentes de tratamento deverão demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, inclusive da eficácia das medidas"[137]. Contudo, a LGPD não foi didática ao tratar da responsabilidade civil do Estado no caso de dano decorrente do tratamento de dados pessoais. Em seus artigos 31 e 32, na Seção intitulada como "Responsabilidade", limita-se a tratar de diretrizes genéricas para Autoridade Nacional de Proteção de Dados:

> Art. 31. Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação.
> Art. 32. A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

---

[136] ZARDO, Francisco. As sanções administrativas de multa simples e multa diária na LGPD. *In*: DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes (coords.). *LGPD & Administração Pública*. São Paulo: Thomson Reuters Brasil, 2020. p. 701.
[137] FEIGELSON, Bruno; SIQUEIRA, Antonio. *Comentários à Lei Geral de Proteção de dados.* São Paulo: Thompson Reuters Brasil, 2019. p. 43-44.

Ou seja, apesar do título, a Seção I do Capítulo IV, da LGPD, não dispõe de forma direta como se dará a responsabilidade civil e penal do ente de Direito Público ao infringir a lei, causando dano ao titular de dados. O capítulo específico das sanções, Seção I do Capítulo VIII da LGPD, limita-se a prever as sanções administrativas decorrentes da violação aos direitos nela consagrados.

Já seu capítulo VI, dispõe sobre a responsabilidade e o ressarcimento dos danos. Ainda que no referido capítulo não faça qualquer menção ao Poder Público, é evidente que possa ser aplicada já que é cláusula geral e está voltada aos agentes de tratamento (controlador e operador), conforme prevê o art. 42, da LGPD[138]. Trata-se de medidas para assegurar a efetiva reparação (§1º), além de apontar dois tipos de relações jurídicas que trarão consequências na responsabilidade civil: "i) uma entre o controlador e operador; ii) outra entre os agentes de tratamento com o titular de dados"[139]. Na primeira hipótese, a previsão legal acerca da solidariedade aponta para a necessidade de que, além do exercício das boas práticas estabelecidas em lei, os controladores saibam escolher bons operadores.[140] Em consonância com o artigo 932, III, do Código Civil "o empregador ou comitente, por seus empregados, serviçais e prepostos, no exercício do trabalho que lhes competir, ou em razão dele." Ademais, a solidariedade é um grande fator para o exercício da segunda hipótese, já que auxilia na identificação do polo passivo da demanda.[141]

---

[138] Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
§1º A fim de assegurar a efetiva indenização ao titular dos dados:
I. o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
II.os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.
§2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar lhe excessivamente onerosa.
§3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.
§4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

[139] TORCHIA, Bruno Martins; MACHADO, Tacianny Mayara Silva. A reponsabilidade subjetiva prevista ne lei geral de proteção de dados e a relação jurídica centre controlador e o encarregado de proteção de dados. *In*: DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes (coords.). *LGPD & Administração Pública*. São Paulo: Thomson Reuters Brasil, 2020. p. 833.

[140] TORCHIA, Bruno Martins. MACHADO, Tacianny Mayara Silva. A reponsabilidade subjetiva prevista ne lei geral de proteção de dados e a relação jurídica centre controlador e o encarregado de proteção de dados. In: DAL POZZO, Augusto Neves E MARTINS, Ricardo Marcondes (coords.). LGPD & Administração Pública. São Paulo: Thomson Reuters Brasil, 2020. P. 836.

[141] Ibidem.

O artigo 42 da LGPD também reforça a regra do Código de Processo Civil relativa à possibilidade de inversão do ônus da prova, que dependerá do caso concreto mediante análise da verossimilhança das alegações e hipossuficiência para fins de prova (§ 2º e artigo 373, § 1º do CPC). No caso do Poder Público, este responde objetivamente pelos danos causados, hipótese em que, habitualmente, o ônus da prova é invertido. Porém, na prática, isso não exime o Autor da ação (titular dos dados ou seu representante no caso de tutela coletiva) de provar o fato constitutivo do direito.[142] Portanto, ao tratar da responsabilidade civil do Poder Público, é possível concluir que a LGPD não a tratou de forma específica, motivo em que deve ser aplicado as regras gerais trazidas pela LGPD, conforme já apresentadas, juntamente com outros dispositivos normativos, que atestam a responsabilidade objetiva do Poder Público em responder por seus atos e danos causados.

Já em relação à Autoridade Nacional de Proteção de Dados (ANPD) é possível concluir que, permanecendo como uma Entidade da Administração Pública Federal Indireta vinculada à Presidência da República, terá enfraquecida sua autoridade diante de agentes e órgãos do Poder Público, adentrando aqui o Poder Judiciário e, portanto, poderá ser gerado grande risco de violação da LGPD, motivo que foi de grande relevância à aprovação da recente Medida Provisória nº 1.124/22, transformando-a em autarquia especial, desvinculada da Presidência da República. Contudo, foi possível observar que a LGPD não ter trazido punição efetiva e sancionadora ao Poder Público nos casos de violação das regras de proteção de dados pode servir como estímulo para o não cumprimento da lei, motivo em que a ANPD precisará utilizar de forma mais severa as demais medidas fiscalizatórias e de penalização autorizadas pela lei ao Poder Público a fim de dar efetividade à norma.

---

[142] AGRAVO INTERNO NO AGRAVO EM RECURSO ESPECIAL. CIVIL E PR OCESSUAL CIVIL. DIREITO DO CONSUMIDOR. COMPRA E VENDA DE IMÓVEL. DEMORA NA BAIXA DE HIPOTECA. DANO MORAL. DECISÃO MONOCRÁTICA DO RELATOR. NULIDADE. INEXISTÊNCIA. NULIDADE DE JULGAMENTO. AUSÊNCIA DE PREQUESTIONAMENTO. SÚMULAS 282 E 356 DO STF. INVERSÃO DO Ô NUS DA PROVA. NECESSIDADE DE COMPROVAÇÃO MÍNIMA DOS FATOS ALEGADOS. SÚMULA 83/STJ AGRAVO INTERNO DESPROVIDO. 3. "A jurisprudência desta Corte Superior se posiciona no sentido de que a inversão do ônus da prova não dispensa a comprovação mínima, pela parte autora, dos fatos constitutivos do seu direito" (AgInt no Resp 1.717.781/RO, Rel. Ministro Marco Aurélio Bellizze, Terceira Turma, julgado em 05/06/2018, DJe de 15/06/2018).4. Agravo interno não provido. (AgInt no AREsp 862.624/RJ, Rel. Ministro Raul Araújo, Quarta Turma, julgado em 22/06/2020, DJe 01/07/2020). BRUNO, Marcos Gomes da Silva. Dos agentes de tratamento de dados pessoais. MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). LGPD: Lei Geral de Proteção de dados comentada. São Paulo: Thomson Reuters Brasil, 2019. p. 319.

4.3 DAS MEDIDAS RESTRITIVAS DE ACESSO AOS DADOS E DOCUMENTOS PESSOAIS NOS PROCESSOS JUDICIAIS ELETRÔNICOS

4.3.1 O método da Pseudonimização como meio de proteção dos dados pessoais expostos nas decisões judiciais e jurisprudência

Os sistemas de consulta de jurisprudência permitem a realização de pesquisas textuais instantâneas em vastos repositórios de sentenças, decisões e acórdãos nos quais geralmente os nomes das partes e de seus/suas advogados(as) são armazenados de forma estruturada e podem ser objeto de consulta específica. Todo esse manancial de informações processuais é consumido por organizações privadas que utilizam mecanismos de coleta automatizada de dados (*web scraping*), sistematizam as informações extraídas para fins comerciais e, muito comumente, disponibilizam os dados estruturados na própria rede mundial de computadores para consulta pública. Diante dessa profusão de vias de acesso às informações processuais torna-se bastante clara a magnitude do desafio de evitar a divulgação de dados pessoais contidos em decisões judiciais.

Assim, a LGPD fez questão de dedicar um capítulo próprio (Capítulo IV) para tratar do tratamento de dados pessoais pelo Poder Público, justamente por reconhecer suas peculiaridades para exercer tal função. A LGPD autoriza o setor público a realizar operações de tratamento de dados de pessoas naturais, independentemente do consentimento dos respectivos titulares, "para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público" (art. 23).

Trata-se da base normativa que, nesse microssistema de proteção de dados, ampara a divulgação pelos tribunais de decisões judiciais que contenham dados pessoais (inclusive sensíveis e independentemente de consentimento) por meio de suas ferramentas de consulta pública disponíveis na rede mundial de computadores. No entanto, essa publicização de decisões judiciais deve observar os princípios gerais sobre tratamento de dados pessoais previstos na LGPD, nomeadamente: finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação; e responsabilização e prestação de contas (art. 6º). Além da utilização dos princípios trazidos pela LGPD para o tratamento de dados pessoais, é necessária a utilização imediata de outros métodos mais eficazes para a proteção de dados pessoais,

como os da omissão, pseudonimização e segredo de justiça como forma de evitar a exposição desses dados em despachos, decisões, sentenças, relatórios, votos, ementas e textos congêneres judiciais, aos quais serão apresentados a seguir. Mas antes, é importante conceituar dado pessoal e pseudonimização para, após, tratar melhor sobre esses métodos.

Dado pessoal é, nos termos da LGPD, toda "informação relacionada a pessoa natural identificada ou identificável" (art. 5º, I). Já a pseudonimização consiste no "tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro" (art. 13, § 4º). Diante desses conceitos, os textos judiciais podem veicular dados pessoais apenas quando indispensáveis e, mesmo nessas situações, devem se valer, tanto quanto possível, de técnicas de pseudonimização a fim de despersonalizá-los, isto é, quebrar o elo entre as informações e as pessoas naturais a que elas se referem. A mero título de ilustração, possíveis estratégias de pseudonimização são:

> • a substituição de nomes próprios completos por suas iniciais (ex.: de José da Silva Pereira para J.S.P);
> • a referência aos papéis processuais desempenhados pelos titulares dos dados (ex.: o autor, a ré, a testemunha, o perito, a recorrente, o agravante) em vez de menções a seus nomes próprios;
> • a supressão parcial de caracteres de modo a inviabilizar a individualização de dados (ex.: e-mail vic...@gmail.com; telefone (61) XXXXX-X983; CPF 019.XXX.XXX-15; CEP 73.025-XX8; placa JIP-XX48);
> • a generalização de informações (ex.: residente na SQN 218, Bloco Z, Apartamento 701, Asa Norte, Brasília-DF para residente na Asa Norte, Brasília-DF; de servidor efetivo do Conselho Nacional de Justiça para servidor público federal)[143].

Contudo, por mais que a técnica da pseudonimização seja de grande valia para a proteção dos dados pessoais, uma parcela dos doutrinadores defendem que não se revela juridicamente admissível a omissão ou pseudonomização automática e generalizada de dados pessoais contidos em decisões judiciais já publicizadas, por entenderem que no sistema judicial brasileiro o afastamento da regra da publicidade dos atos processuais se submete à reserva de jurisdição. Cabe, portanto, aos(às) magistrados(as), e

[143] CONSELHO NACIONAL DE JUSTIÇA. Tratamento de dados pessoais na consulta de jurisprudência: desafio e perspectivas. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2022/02/tratamento-dados-pessoais-consulta-jurisprudencia30-11-21.pdf. Acesso em: 29 nov. 2022.

exclusivamente a eles(as), diante das circunstâncias particulares de cada caso concreto, realizar o juízo de necessidade sobre a publicização de dados pessoais.

Contudo, esse entendimento não deve prevalecer. Caso aplicado o juízo de necessidade pelo magistrado, nem sempre o cuidado dispensado na redação ou edição dos textos judiciais publicizados será suficiente para impedir a disseminação dos dados pessoais. Além do mais, não cabe ao magistrado ter essa autonomia em avaliar e determinar qual dado pessoal deve ser ou não protegido por um dos métodos mencionados, pois as normas da LGPD, demais normas infraconstitucionais e a própria Constituição Federal, no inciso LXXIX do artigo 5º, garantem proteção a todo e qualquer dado pessoal. Logo, todo dado pessoal deve ser protegido conforme a Carta Magna e, por isso, uma vez que a CF e demais normas infraconstitucionais não especificaram quais dados pessoais merecem ou não proteção, não cabe ao magistrado fazer essa avaliação. Portanto, o mais correto a se fazer para que os tribunais possam alcançar a efetividade das normas da LGPD e garantir proteção aos direitos fundamentais da intimidade e privacidade, é desenvolver e aplicar métodos de proteção a todos os dados pessoais, sem distinção.

Nesse sentido, quanto às decisões judiciais e jurisprudência que já foram publicizadas, a alternativa seria fazer a omissão ou pseudonomização de forma automática e generalizada em todos os dados pessoais através de ferramentas de *softwares*. Para isso, é indispensável a adaptação da infraestrutura tecnológica do Poder Judiciário, a fim de admitir a coexistência de versões diferentes de um mesmo texto judicial, com diferenciação dos perfis autorizados a consultar cada uma delas. Ou seja, para que dados pessoais possam ser devidamente omitidos ou pseudonimizados após a publicização das decisões judiciais que os contêm é indispensável que os sistemas processuais e de divulgação de jurisprudência viabilizem a convivência de versões integrais das decisões judiciais (acessíveis exclusivamente às partes do processo), de um lado, com versões editadas desses mesmos textos (disponíveis para consulta pública de terceiros), de outro.

Destaca-se que o Conselho Nacional de Justiça, através dos estudos realizados pelo Comitê de Apoio para Elaboração de Estudos e Pareceres Técnicos sobre a Sistematização do Serviço de Jurisprudência no Poder Judiciário[144], emitiu parecer com

[144] CONSELHO NACIONAL DE JUSTIÇA. Tratamento de dados pessoais na consulta de jurisprudência: desafio e perspectivas. 2022. Disponível em: https://www.cnj.jus.br/wp-

alguns complementos a essas medidas, entendendo que os tribunais podem considerar a implementação de dois ajustes pontuais com o condão de atenuar o alcance da exposição dos dados pessoais e minimizar os danos dela decorrentes.

O primeiro ajuste diz respeito à estrutura dos bancos de jurisprudência. Comumente, as bases jurisprudenciais armazenam, de forma estruturada, os dados de identificação das partes e de seus/suas advogados(as), de modo a viabilizar que os(as) usuários(as) dos sistemas de consulta possam resgatar documentos utilizando dessas informações específicas. A supressão dos dados estruturados de identificação de partes e advogados(as) poderia contribuir para romper o elo entre as informações pessoais contidas nos documentos e os titulares desses dados. Aplicada de forma geral a todos os registros do banco de jurisprudência, a eliminação dessas informações atuaria, portanto, como uma medida de pseudonimização de dados pessoais.

Numa abordagem menos agressiva, em vez da mera supressão, os dados estruturados de identificação de partes e advogados(as) poderiam ser mantidos no banco de jurisprudência, aplicando-se a eles técnicas de pseudonimização (como o registro apenas das letras iniciais dos nomes) quando relacionados a pessoas naturais (não a pessoas jurídicas)[145]. Outra alternativa à simples supressão seria conservar nas bases de dados os dados estruturados de identificação, mas não os indexar para fins de busca. Nessa linha, as informações continuariam a ser exibidas, de forma passiva, quando da apresentação dos resultados, mas caso um(a) usuário(a) informasse os dados de identificação ativamente em sua expressão de busca (argumento de pesquisa) os documentos não seriam recuperados[146].

Em qualquer dessas vertentes (supressão, pseudonimização ou não indexação de informações), as modificações relativas aos dados estruturados de identificação de partes e advogados(as) encontram amparo na Resolução n.º 121, de 2010, do Conselho Nacional de Justiça, segundo a qual "a disponibilização de consultas às bases de decisões judiciais impedirá, quando possível, a busca pelo nome das partes" (art. 5º). Ainda assim, o Comitê de Apoio para Elaboração de Estudos e Pareceres Técnicos sobre a Sistematização do Serviço de Jurisprudência do CNJ deram atenção aos cabeçalhos de identificação de

content/uploads/2022/02/tratamento-dados-pessoais-consulta-jurisprudencia30-11-21.pdf. Acesso em 29 nov. 2022.

[145] CONSELHO NACIONAL DE JUSTIÇA. Tratamento de dados pessoais na consulta de jurisprudência: desafio e perspectivas. 2022.

[146] CONSELHO NACIONAL DE JUSTIÇA. Tratamento de dados pessoais na consulta de jurisprudência: desafio e perspectivas. 2022.

partes e advogados(as) contidos nos textos das decisões judiciais. Tradicionalmente, os próprios arquivos de texto dos acórdãos, das decisões e das sentenças contêm cabeçalhos destinados a indicar as partes e advogados(as) relacionados aos feitos apreciados. Em geral, essas informações são incluídas de forma automática pelos programas de edição de texto utilizados pelos tribunais. Em razão da existência desses cabeçalhos, os sistemas de consulta de jurisprudência que admitem pesquisa na íntegra (inteiro teor) dos documentos acabam possibilitando, por tabela, que os usuários(as) recuperem julgados com base em dados identificadores de partes e advogados(as).

Além disso, os arquivos de acórdãos, decisões e sentenças são coletados e processados de forma automática e em escala, por terceiros que, com facilidade, podem estabelecer a conexão entre as informações pessoais contidas nos documentos e as pessoas naturais identificadas nos respectivos cabeçalhos. Nesse contexto, um possível ajuste a considerar seria simplesmente abolir dos textos judiciais os cabeçalhos de identificação de partes e advogados(as) ou, alternativamente, aplicar-lhes técnicas de pseudonimização (como o registro apenas das letras iniciais dos nomes) de forma generalizada[147].

Nesse contexto, vale mencionar alguns países europeus, mais especificamente, a França, Itália e Alemanha, que já estão mais avançados no tema proteção de dados pessoais e já aplicam os métodos apresentados e outros em seus Tribunais de Justiça que poderão servir como exemplo para o ordenamento jurídico brasileiro. No tocante ao sistema francês, as recentes modificações introduzidas pela Lei 2019-222[148], que dispõe sobre a reforma do Judiciário, chamaram atenção da comunidade jurídica mundial, ao prever a anonimização de todas as informações pessoais dos magistrados e servidores, de modo a impossibilitar uma predição jurisdicional. A providência francesa não restringiu o acesso público às informações processuais. Ao contrário, teve a intenção de regulamentar a proteção dos dados pessoais das partes, a ocultação dos nomes dos magistrados e dissuadir a prática de reutilização dessas informações, inclusive para fins comerciais. Na França, todos os elementos passíveis de identificação do indivíduo, enquanto parte no processo judicial, como nome, cadastro público, endereço, data de

[147] CONSELHO NACIONAL DE JUSTIÇA. Tratamento de dados pessoais na consulta de jurisprudência: desafio e perspectivas. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2022/02/tratamento-dados-pessoais-consulta-jurisprudencia30-11-21.pdf. Acesso em 29 nov. 2022.
[148] FRANÇA. Loi nº 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice. Paris: Légifrance, 2019. Disponível em: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000038261631/. Acesso em: 16 jun. 2022.

nascimento e outros, assim como informações sensíveis ou não, que possam levar a reidentificação do sujeito pelo cruzamento de dados, são ocultados antes de serem disponibilizados ao público, o mesmo ocorrendo com as informações constantes das decisões, que sofrem o processo de anonimização, antes de serem repassados a terceiros[149].

A Itália, sem se descurar da publicidade dos autos judiciais, também estabeleceu o critério de anonimização de informações "relativas à qualificação das partes e de seus advogados, bem como detalhes dos autos dos quais seja possível extrair informações de caráter pessoal e reservado, ainda que por meio de pesquisa em outros bancos de dados"[150]. Na Alemanha, os indivíduos não têm acesso às decisões ou sentenças, senão quando são proferidas oralmente, não sendo possível a obtenção de certidões, cópias ou registro documentais, mas apenas um conjunto de decisões disponibilizadas em sítio eletrônico do tribunal e, ainda assim, após a anonimização de todos os dados passíveis de identificação dos sujeitos do processo[151].

Não obstante a restrição inicial, o sistema alemão admite o acesso de terceiros aos autos judiciais se e quando demonstrada o legítimo interesse na informação, sendo que com relação aos autos eletrônicos, mesmo que comprovado o legítimo interesse, o acesso só poderá ocorrer nos terminais de consulta do respectivo tribunal, sendo possível somente a extração de cópias impressas das informações processuais, mesmo que os autos sejam digitalizados[152].

A análise pragmática levada a efeito pela Associação Lawgorithm, Associação de Pesquisa em Inteligência Artificial e Direito, fundada por professores das faculdades de Direito, Engenharia, Matemática e Filosofia da Universidade de São Paulo[153], teve em conta uma radiografia do Judiciário europeu, com indicadores de transparência, da acessibilidade de decisões *on-line* ao público em geral, da qualidade da informação

---

[149] FRANÇA. Loi nº 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice. Paris: Légifrance, 2019.

[150] CUEVAS, Ricardo Villas Boas. Anonimização e Pseudonimização de Dados Pessoais no Processo Eletrônico. *In*: TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. *O Direito Civil na era da Inteligência*. São Paulo: Thomson Reuters Brasil, 2020. p. 258.

[151] MARANHÃO, Juliano de Souza Albuquerque (coord.). *Acesso a dados de processos judiciais no Brasil*. São Paulo: Associação Lawgorithm de Pesquisa em Inteligência Artificial, 2020. Disponível em: https://lawgorithm.com.br/wp-content/uploads/2020/07/ReportAcessoDadosJudiciário.pdf. Acesso em: 16 jun. 2022.

[152] MARANHÃO, Juliano de Souza Albuquerque (coord.). *Acesso a dados de processos judiciais no Brasil*. São Paulo: Associação Lawgorithm de Pesquisa em Inteligência Artificial, 2020.

[153] MARANHÃO, Juliano de Souza Albuquerque (coord.). *Acesso a dados de processos judiciais no Brasil*. São Paulo: Associação Lawgorithm de Pesquisa em Inteligência Artificial, 2020.

disponibilizada e acessada e sua adequação ao Regulamento Geral de Proteção de Dados europeu[154]. Nesse tópico, a maior compatibilidade foi medida pelo uso do método de anonimização dos dados pessoais das partes que, antes de 2016, era empregada em graus e formas discrepantes entre as instâncias judiciais e os países-membros, mas ainda assim acolhida por padrão pela maioria dos Estados, em atenção ao direito fundamental de privacidade e autodeterminação informacional, o que motivou o aprimoramento, pela uniformização do acesso aos dados judiciais. Portanto, as experiências internacionais relatadas acima indicam a evolução na mudança de paradigma na concepção do direito à privacidade, que não mais se limita ao oculto, ao segredo ou ao privado, propriamente dito, mas, sim, ao controle, à proteção, à segurança, à regulação do trânsito e tratamento das informações.

Como um direito fundamental agregado ou independente da garantia constitucional à vida privada a proteção de dados pessoais só será efetivada se as práticas de tratamentos de dados mostrarem-se próprias para a proteção desse direito. Não obstante a própria Lei nº 13.709/2018 não afastar incidentes de segurança que possam decorrer de métodos inovadores de acesso cibernético não autorizado, é também a referida lei brasileira que determina aos controladores dos dados a adoção de medidas preventivas, que minimizem os impactos de eventual incidente[155].

4.3.2 A Autodeterminação Informativa do titular do dado como método para instituir o Segredo de Justiça a seus dados e documentos pessoais em um processo judicial eletrônico

Além dos métodos apresentados acima, o segredo de justiça é um dos institutos mais eficazes para a proteção de dados pessoais no âmbito de um processo judicial eletrônico, e ao ser adotada a autodeterminação informativa do titular do dado para a aplicação desse instituto (direito que cada indivíduo tem de controlar e proteger seus

---

[154] UNIÃO EUROPEIA. Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). [S. l.]: EUR-Lex, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 16 jun. 2022.

[155] PELLEGRINO, Maria Cristina Conde. *DA MIHI DATA, DABO TIBI JUS*: o tratamento de dados pessoais no âmbito do processo judicial eletrônico brasileiro, à luz da Lei Geral de Proteção de Dados' 13/07/2021 147 f. Dissertação (Mestrado em Instituições Sociais, Direito e Democracia) - UNIVERSIDADE FUMEC, Belo Horizonte Biblioteca Depositária: FCH, 2021.

dados pessoais), mais eficaz se torna essa proteção. Atualmente, a publicidade processual é concretizada através de diversos pontos de acesso mantidos pelos tribunais na rede mundial de computadores. Os dados básicos de todos os processos, como os nomes das partes e de seus advogados, número de CPF, assim como o inteiro teor das decisões, sentenças e acórdãos estão disponíveis para consulta pública por meio dos sistemas de acompanhamento processual, independentemente de prévio cadastramento ou de demonstração de interesse (arts. 1º, 2º e 4º da Resolução CNJ n.º 121, de 2010, do Conselho Nacional de Justiça).

As peças processuais que compõem os autos dos processos eletrônicos, que também possuem vários dados sensíveis, como nome, CPF, RG, estado civil, filiação, data de nascimento, endereço residencial, telefone de contato, além de vários outros documentos pessoais que envolvem a privacidade e intimidade das partes, estão acessíveis a quaisquer advogados(as), procuradores(as) ou membros do Ministério Público, ainda que não vinculados(as) ao caso específico (art. 11, § 7º, da Lei nº n. 11.419, de 2006). A íntegra de sentenças e decisões, bem como as ementas dos acórdãos, são publicadas no Diário da Justiça eletrônico (art. 4º da Lei nº n. 11.419, de 2006; art. 205, § 3º, do Código de Processo Civil), que deve obrigatoriamente indicar o nome completo, sem abreviaturas, das partes e de seus/suas advogados(as) (art. 272, §§ 2º e 3º, do Código de Processo Civil). Ocorre que o princípio da publicidade não foi idealizado para publicizar informações pessoais dos sujeitos do processo, como nome, endereço, números cadastrais e outros, mas sim para difundir a informação sobre o ato jurisdicional, de modo que a sociedade possa se certificar da obediência ao devido processo constitucional.

Nesse prisma, para tornar efetiva a proteção dos dados pessoais nos processos judiciais nas hipóteses em que não bastarem a simples omissão ou a mera pseudonimização, métodos abordados no tópico anterior, é possível recorrer ao instituto do segredo de justiça. Muito antes do advento da LGPD, o segredo de justiça já cumpria, em algumas situações, a função de limitar o acesso de terceiros (estranhos aos processos) a dados pessoais. Mais do que isso: ao passo que as medidas de digitalização e ampliação do acesso a informações processuais foram implementadas, o Poder Judiciário foi construindo paulatinamente o arcabouço regulamentar e a infraestrutura tecnológica necessários ao resguardo dos processos que tramitam sob segredo de justiça.

Dessa forma, em casos submetidos ao segredo de justiça, os sistemas de acompanhamento processual não divulgam ao público dados, como os nomes das partes, seus números de identificação no cadastro federal de contribuintes ou o inteiro teor das

decisões, sentenças e acórdãos (art. 1º, parágrafo único, da Resolução CNJ n.º 121, de 2010, do Conselho Nacional de Justiça). Além disso, em casos de segredo de justiça, o acesso às peças processuais e demais documentos juntados fica condicionado à existência de vínculo específico do(a) interessado(a) com o processo (art. 3º, § 1º, da Resolução CNJ n.º 121, de 2010; e art. 27, caput, da Resolução CNJ nº n. 185, de 2013; ambas do Conselho Nacional de Justiça; art. 11, §§ 6º e 7º, da Lei n.º 11.419, de 2006; art. 107, I, e art. 189, § 1º, do Código de Processo Civil). Adicionalmente, nos processos que tramitam sob segredo de justiça, é praxe a pseudonimização dos cabeçalhos de identificação, tanto nas publicações do Diário da Justiça, quanto nos registros dos repositórios de jurisprudência, nos quais os atos publicizados são identificados costumeiramente apenas pelas letras iniciais dos nomes das partes (e não por seus nomes completos).

Ao detalhar as exceções à publicidade processual, o legislador ordinário incluiu entre as hipóteses que autorizam a imposição de segredo de justiça as situações "em que o exija o interesse público ou social" e "em que constem dados protegidos pelo direito constitucional à intimidade" (art. 189, I e III, do Código de Processo Civil). Trata-se de cláusulas gerais suficientemente abertas para viabilizar o resguardo das informações processuais em situações não antevistas, de modo específico e explícito, pela legislação.

Além das hipóteses genéricas relacionadas à intimidade e ao interesse público e social, cabe relembrar que a legislação ordinária prevê, de forma específica, uma série de outras situações que justificam a decretação de segredo de justiça como medida de proteção de dados pessoais, entre as quais se destacam as seguintes: Casamento, separação de corpos, divórcio, separação, união estável - art. 189, II, do Código de Processo Civil; Filiação, alimentos e guarda de crianças e adolescentes - art. 189, II, do Código de Processo Civil; Reconhecimento do estado de filiação - art. 27 do Estatuto da Criança e do Adolescente; Alimentos para filhos(as) havidos fora do casamento - art. 1.705 do Código Civil; Crimes contra a dignidade sexual - art. 234-B do Código Penal; Exposição do ofendido aos meios de comunicação - art. 201, § 6º, do Código de Processo Penal; Pena extinta ou cumprida - art. 202 da Lei de Execução Penal; Crianças e adolescentes a que se atribua autoria de ato infracional - art. 143 do Estatuto da Criança e do Adolescente; Interceptação de comunicações telefônicas - art. 1º da Lei nº n. 9.296, de 1996; Alteração do nome de vítima ou testemunha sob proteção - art. 9º, § 2º da Lei nº n. 9.807, de 1999; Registros de conexão e de acesso a aplicações de internet - art. 23 da Lei nº n. 12.965, de 2014; Arbitragem com confidencialidade comprovada - art. 189, IV, do Código de Processo Civil; art. 22-C, parágrafo único, da Lei n. 9.307, de 1996.

Diante das hipóteses acima os casos específicos taxados por lei poderão ser instituídos pelo Segredo de Justiça de forma automática ao ser distribuída a ação judicial. Já nas hipóteses que envolvem à intimidade e privacidade da parte, na grande maioria dos processos, cabe à própria parte, através de seu patrono, requerer o instituto do Segredo de Justiça ao qual será avaliado pelo magistrado, deferido ou não. Ou seja, o magistrado que fará essa análise se caberá ou não o instituto do segredo de justiça àquele processo judicial. Ocorre que, como já visto no tópico anterior, a autonomia dada aos magistrados em avaliar e decidir que referido processo deve permanecer ou não em segredo de justiça por possuir ou não dados pessoais que violam o direito à intimidade da parte, vai contra as normas da LGPD e da própria Constituição Federal que determinam a proteção a qualquer dado pessoal, sem distinção e diferenciação dos mesmos. Além do mais, conforme já visto no capítulo anterior, os direitos à privacidade e intimidade ganharam, ao longo do tempo, grande amplitude em seu conceito e alcance. Logo, os dados pessoais que correspondem à privacidade e intimidade das partes são amplos e não possuem rol taxativo, o que dificulta mais ainda essa análise de proteção pelo magistrado.

Nesse sentido, como solução à questão apresentada, se faz necessário analisar um método eficiente a ser aplicado no sistema do Processo Judicial Eletrônico (PJE) e todos os demais sistemas eletrônicos do judiciário, que seja possível dar autonomia para o titular do dado pessoal controlar, através do instituto de segredo de justiça, todos seus dados e documentos pessoais presentes em um processo judicial, sem necessidade de deferimento ou não do magistrado, porém, podendo impugnar, em momento posterior, método que será abordado a seguir.

Com o processo eletrônico, a distribuição do processo é feita pelo próprio advogado. No momento do cadastro e inclusão dos documentos ele pode marcar, por exemplo, a urgência do pedido, tendo ciência no mesmo ato para qual Juízo foi distribuído. Em questão de horas ou minutos, após a distribuição, o processo já pode estar concluso. A distribuição far-se-á com a petição inicial que será cadastrada através do login de um advogado, procurador ou *jus postulandi*, sendo que é ele que irá definir a especialidade, assunto, se o processo deve se encontrar em segredo de justiça ou não, qualificação das partes, anexar a petição e a documentação. Ao final, o processo é criado e será automaticamente distribuído para um dos juízos da 1ª Instância[156].

[156] CONSELHO NACIONAL DE JUSTIÇA. Tratamento de dados pessoais na consulta de jurisprudência: desafio e perspectivas. 2022. Disponível em: https://www.cnj.jus.br/wp-

Em relação à juntada de documentos com o processo eletrônico, da mesma forma como o processo é distribuído de forma automática, toda petição ou documento é juntado ao processo também de forma automatizada. Se houver erro de juntada, cabe à Vara excluir ou cancelar o evento de juntada do documento. Ao estabelecer normas sobre o processo judicial eletrônico, a Resolução n.º 185, de 2013, do Conselho Nacional de Justiça, prevê a possibilidade de as partes indicarem a hipótese de segredo de justiça já no momento do protocolo de suas petições, bem como garante que, nessas situações, os autos tramitarão em segredo até eventual deliberação em sentido contrário do(a) magistrado(a) responsável (art. 28, caput e §§ 1º e 2º)[157].

Desse modo, conforme a análise procedimental do ajuizamento de um processo judicial, uma boa alternativa de método a ser utilizado pelo titular do dado para restringir a exposição de dados pessoais nos processos judiciais (sejam eles sensíveis ou não) é pelo método da Autodeterminação Informativa, que seria o próprio titular do dado pessoal, através do advogado ou outro membro do judiciário que o defenda, ter a possibilidade de controle dos seus próprios dados dentro do sistema de um processo judicial eletrônico, sendo permitido selecionar a opção de "Segredo de Justiça – Dado Pessoal - LGPD" para cada protocolo de petição e/ou juntada de documentos que contenham dados pessoais, ou então, por meio de edição daquele dado ou documento pessoal já disponível ou publicizado para que fique em segredo de justiça.

Com a aplicação desse método, qualquer dado ou documento pessoal presente em um processo judicial, que não esteja já em segredo de justiça, permanecerá em sigilo, apenas acessível às partes, advogados e magistrados vinculados diretamente ao processo judicial, assim como não ferirá o direito fundamental à publicidade dos atos processuais, pois nos processos em que não estiverem em segredo de justiça, o acesso a todos os atos processuais estarão disponíveis, sem restrição, permanecendo apenas os dados e documentos pessoais da parte em sigilo.

Por fim, as consequências da aplicação do método da Autodeterminação Informativa pelo titular do dado para instituir de forma autônoma e automática a proteção de seus dados pessoais pelo instituto do segredo de justiça em um processo judicial serão: o magistrado perder a autonomia de decidir quais dados pessoais que integram à

content/uploads/2022/02/tratamento-dados-pessoais-consulta-jurisprudencia30-11-21.pdf. Acesso em 29 nov. 2022.

[157] CONSELHO NACIONAL DE JUSTIÇA. Tratamento de dados pessoais na consulta de jurisprudência: desafio e perspectivas. 2022.

privacidade e intimidade das partes devem ser ou não protegidos pelo instituto de segredo de justiça; fazer com que apenas as partes, os advogados e magistrados vinculados ao processo tenham acesso a esses dados pessoais; garantir ao Judiciário mais efetividade às normas da LGPD e respeito aos direitos fundamentais da intimidade e privacidade dos cidadãos.

Nesse contexto, é possível apresentar como exemplo o Sistema Eletrônico de Informações (SEI), que já aplica esse método desde abril de 2022. O SEI é um sistema de produção e gestão de documentos e processos eletrônicos, cedido de maneira gratuita à administração pública. O sistema foi desenvolvido pelo Tribunal Regional Federal da 4ª Região (TRF4) e selecionado como o recurso de processo eletrônico no contexto do projeto Processo Eletrônico Nacional (PEN)[158]. Como garantia de fornecerem efetividade na proteção de dados pessoais, respeitando as normas previstas pela LGPD, a privacidade e intimidade do cidadão, incluíram dentro do seu sistema a possibilidade da própria parte, titular do dado, efetuar edição de um documento interno, selecionando o dado pessoal ou dado pessoal sensível a ser preservado através da opção de restrição de acesso devido às normas da LGPD. Com o procedimento, os dados a serem tratados serão visíveis apenas na unidade geradora do documento[159]. O referido sistema serve de exemplo ao Poder Judiciário na aplicação do método apresentado acima.

Portanto, diante do exposto, não se pode ignorar que a publicização de dados pessoais e sensíveis presentes em processos judiciais apresenta grande potencial de lesão a direitos fundamentais, a recomendar cuidado adicional, devendo ser seriamente considerada a possibilidade de impor segredo de justiça a esses dados e documentos pessoais, com fundamento nas normas da Lei Geral de Proteção de Dados, no direito à intimidade trazido pelo art. 189, III, do Código de Processo Civil e à própria CF. Para isso, a possibilidade do próprio titular do dado pessoal exercer seu direito de Autodeterminação Informativa e ter autonomia para decretar segredo de justiça à determinado dado ou documento pessoal dentro de um processo judicial, traz o condão de ativar camadas adicionais de proteção aos dados pessoais, preservando os direitos da

[158] LGPD BRASIL. Novo módulo de consulta pública do Sei deve iniciar a partir de Abril. Acessível em: https://www.lgpdbrasil.com.br/novo-modulo-de-consulta-publica-do-sei-deve-iniciar-a-partir-de-abril/. Acessado em 06. Dez 2022.
[159] UNIVERSIDADE FEDERAL DO PARANÁ. Ferramenta do SEI! vai ajudar na proteção de dados: veja como usar. Acessível em: https://www.ufpr.br/portalufpr/noticias/ferramenta-do-sei-vai-ajudar-na-protecao-de-dados-pessoais-veja-como-usar/. Acessado em: 06. dez. 2022.

privacidade e intimidade do cidadão e trazendo mais efetividade às normas da LGPD ao Poder Judiciário.

5 CONCLUSÃO

A evolução acelerada das tecnologias de armazenamento, processamento e compartilhamento de dados amplificou consideravelmente o risco de lesão aos direitos fundamentais à privacidade, à intimidade e ao livre desenvolvimento da personalidade. Mundo afora, as ordens jurídicas têm produzido diferentes instrumentos legais para garantir às pessoas naturais proteção jurídica adequada em face do potencial lesivo das novas tecnologias. A Lei Geral de Proteção de Dados Pessoais se insere nesse quadro global como uma resposta do ordenamento jurídico brasileiro à nova realidade tecnológica.

Nesse contexto, a adaptação dos sistemas do Processo Judicial Eletrônico (PJe), Diário da Justiça Eletrônico (DJe) e demais serviços de divulgação de jurisprudência à LGPD representa um grande desafio para o Poder Judiciário brasileiro, seja porque a tradição jurídica nacional consagra o princípio da publicidade dos atos processuais como regra, seja porque a implementação das mudanças necessárias esbarram em limitações de ordem administrativa, tecnológica e financeira dos tribunais.

Diante desse desafio, o Poder Judiciário deve pautar sua atuação pela lógica possível, privilegiando a adoção de soluções que, sendo razoáveis e exequíveis, mostrem-se capazes de minimizar os riscos de exposição indevida de dados pessoais, sem sacrificar valores constitucionais igualmente relevantes (como a publicidade), nem impor aos tribunais custos administrativos, tecnológicos ou financeiros insuportáveis. Durante o processo de adequação à LGPD, os tribunais devem dedicar especial atenção à mudança da cultura organizacional, a ser concretizada por meio de ações de sensibilização contínuas e abrangentes.

À luz dessas premissas, a seguir serão apresentadas as principais medidas que foram discutidas ao longo do presente trabalho como possíveis caminhos a serem trilhados pelos tribunais com a finalidade de trazer efetividade à proteção de dados pessoais dos cidadãos expostos nos processos judiciais eletrônicos, resguardando os direitos fundamentais da privacidade e intimidade.

Analisando a Lei do Processo Eletrônico, as Resoluções Normativas do CNJ criadas para a adequação dos Tribunais às normas de proteção de dados junto à Lei Geral de Proteção de Dados Pessoais, é possível afirmar que a Lei do Processo Eletrônico não vai de encontro com as regras previstas na LGPD, pelos seus objetivos centrais serem garantir a publicidade e transparência dos atos processuais, como mais acesso à justiça

aos cidadãos, mais acesso aos atos e dados processuais pelos advogados e demais membros do judiciário, sem focar sua atenção na proteção aos dados pessoais expostos nos processos judiciais eletrônicos. No presente trabalho foi possível reconhecer que o direito fundamental da publicidade dos atos processuais é importante para evitar atos abusivos do poder público, oferecendo mais transparência à sociedade, o que não se deve questionar ou criticar o art. 5º, LX, da CF no que se refere à obrigatoriedade da publicidade dos atos processuais. Contudo, é possível afirmar que em nenhum momento a Constituição Federal menciona a obrigatoriedade da publicidade dos dados e documentos pessoais das partes, sendo que ato processual é diferente de dado pessoal. Assim, restringir o acesso aos dados e documentos pessoais processuais de membros internos e externos ao Judiciário que não possuem vínculo direto ao processo em litígio, não infringiria os dispositivos da CF e demais leis infraconstitucionais que garantem a publicidade de atos processuais, pelo contrário, garantirá com muito mais efetividade os direitos fundamentais que envolvem a dignidade da pessoa humana, como a privacidade, intimidade e proteção de dados pessoais.

No que tange às resoluções criadas pelo CNJ, é possível afirmar que são relevantes para a adequação dos Tribunais à LGPD. Porém, não há regulamentação de alcance geral sobre os meios técnicos mais adequados e consentâneos com a melhor tecnologia voltada à segurança do sistema e à prevenção de incidentes de acesso não autorizado. Pelo contrário, limitam-se a transferir essa responsabilidade a cada um dos tribunais brasileiros, sem uma padronização e uniformização. Além do mais, não tratam de métodos de restrição ao livre acesso de terceiros aos milhares de dados pessoais expostos nos processos judiciais eletrônicos, decisões judiciais, jurisprudência e demais serviços de divulgação, pautando-se as resoluções em obrigações genéricas previstas na LGPD. Assim também, ao ser recomendada a divulgação de informações no sítio eletrônico das cortes judiciais (à exceção do Supremo Tribunal Federal) quanto à forma e às obrigações a serem adotadas no tratamento de dados, inexiste a recomendação ou informação voluntária sobre quais providências foram efetivadas e como foram cumpridas. Por tudo isso, é possível concluir que as resoluções criadas pelo CNJ ainda não suprem uma adequação efetiva do Judiciário às normas da LGPD, devendo os pontos apresentados serem revistos pelo órgão.

Partindo para a análise feita dos frequentes ataques maliciosos no Judiciário foi possível observar que o sistema de segurança e prevenção adotados pelos Tribunais ainda são muito frágeis e vulneráveis, motivo que os tornam alvos de ataques, invasões e

atividades maliciosas. Nessa análise foi também verificado que, após esses ataques, não houve esclarecimento pelos Tribunais aos cidadãos sobre o real alcance da violação ou o grau de comprometimento das informações processuais públicas ou sigilosas, indevidamente acessadas. Não houve informação sobre a titularidade dos dados, e quais os dados sequestrados. Não se demonstrou a adoção de medidas eficazes que comprovassem o cumprimento das normas de proteção de dados. Não houve transparência sobre a forma de tratamento de dados, sobre as medidas técnicas e administrativas empregadas na solução do problema, ou, ainda, sobre as medidas preventivas para sustar os danos decorrentes do vazamento, todas condições erigidas no art. 6º da Lei nº 13.709/2018, como princípios a serem observados.

Diante disso, é possível afirmar que a Autoridade Nacional de Proteção de Dados Pessoais (ANPD) deve fiscalizar com mais severidade o Judiciário e aplicar sanções administrativas com mais frequência. Acredita-se, também, que as melhores soluções para evitar essas invasões seria, tanto a LGPD, como as resoluções normativas do CNJ criadas para melhor adequar os Tribunais à lei, estipularem a adoção padronizada de certos sistemas de segurança e prevenção mais avançados, diferente da realidade de hoje, onde cada tribunal tem autonomia para escolher quais sistemas e medidas de segurança devem ser adotados para proteger os dados coletados e armazenados por eles. Para isso, se faz necessário um melhor investimento pelos Tribunais em equipes capacitadas de TI e segurança, em tecnologias mais avançadas, como forma de melhorar a proteção de seus sistemas, assim como aplicar a adoção de boas práticas e governança, que estabeleçam as condições de organização, normas de segurança, padrões técnicos para mitigação de riscos e ações de treinamento sobre a Lei Geral de Proteção de Dados Pessoais destinadas a magistrados(as) e auxiliares da justiça em geral, com foco nos princípios e valores que informam a LGPD e no contexto tecnológico a ela subjacente.

Ainda assim, em análise da LGPD no que se refere ao tratamento de dados pessoais pelo Poder Público, é possível concluir que para qualquer ato que importe em tratamento e compartilhamento de dados pessoais pelo Judiciário, deve observar os princípios elencados no art. 6º da Lei nº 13709 de 2018, com destaque aos princípios da segurança, da prevenção, da responsabilização e prestação de contas, visando a transparência na persecução do interesse público, na execução de competências legais, com a necessária informação da base legal autorizadora do tratamento de dados prevista nos arts. 7º e 11º da LGPD, como o Consentimento Informado, Cumprimento de Obrigação Legal ou Regulatória pelo Controlador, Execução de políticas públicas pela

Administração Pública, Exercício regular de direitos em processo judicial e Legítimo Interesse. Caso violadas as regras de tratamento de dados, mesmo a LGPD não tratando de forma específica sobre a responsabilidade civil do Poder Público, deverá responder conforme as regras gerais trazidas pela LGPD, como as dos arts. 31, 32 e 42, juntamente com outros dispositivos normativos do CC e CPC, que atestam a responsabilidade objetiva do Poder Público em responder por seus atos e danos causados, além de poder receber sanções administrativas da Autoridade Nacional de Proteção de Dados (ANPD). Por mais que a LGPD não tenha trazido a possibilidade da ANPD em aplicar sanção pecuniária ao Poder Público nos casos de violação das regras de proteção de dados, punição essa que seria mais efetiva e sancionadora, agora, a ANPD terá mais autonomia em fiscalizar e aplicar sanções administrativas, uma vez que, devido à recente Medida Provisória nº 1.124/22, foi transformada em autarquia especial, desvinculada da Presidência da República, o que fortalecerá sua autoridade perante os órgãos públicos.

Ademais, com o objetivo de restringir a exposição dos dados pessoais das partes em processos judiciais eletrônicos, foram apresentados no trabalho métodos mais eficazes para essa proteção, como os da pseudonimização em dados pessoais presentes em textos judiciais e da aplicação do instituto do segredo de justiça por meio do direito da autodeterminação informativa do próprio titular do dado.

O método da pseudonimização ("dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro") tem como fim quebrar o elo entre as informações e as pessoas naturais a que elas se referem, como exemplo:

> • a substituição de nomes próprios completos por suas iniciais (ex.: de José da Silva Pereira para J.S.P);
> • a referência aos papéis processuais desempenhados pelos titulares dos dados (ex.: o autor, a ré, a testemunha, o perito, a recorrente, o agravante) em vez de menções a seus nomes próprios;
> • a supressão parcial de caracteres de modo a inviabilizar a individualização de dados (ex.: e-mail vic...@gmail.com; telefone (61) XXXXX-X983; CPF 019.XXX.XXX-15; CEP 73.025-XX8; placa JIP-XX48);
> • a generalização de informações (ex.: residente na SQN 218, Bloco Z, Apartamento 701, Asa Norte, Brasília-DF para residente na Asa Norte, Brasília-DF; de servidor efetivo do Conselho Nacional de Justiça para servidor público federal)[160].

[160] CONSELHO NACIONAL DE JUSTIÇA. Tratamento de dados pessoais na consulta de jurisprudência: desafio e perspectivas. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2022/02/tratamento-dados-pessoais-consulta-jurisprudencia30-11-21.pdf. Acesso em: 29 nov. 2022.

Para isso, uma boa alternativa para as decisões judiciais e jurisprudência que já foram publicizadas seria fazer a omissão ou pseudonomização de forma automática e generalizada em todos os dados pessoais através de ferramentas de *softwares*. Assim, é indispensável a adaptação da infraestrutura tecnológica do Poder Judiciário, a fim de admitir a coexistência de versões diferentes de um mesmo texto judicial, com diferenciação dos perfis autorizados a consultar cada uma delas, ou seja, para que dados pessoais possam ser devidamente omitidos ou pseudonimizados após a publicização das decisões judiciais que os contêm, é indispensável que os sistemas processuais e de divulgação de jurisprudência viabilizem a convivência de versões integrais das decisões judiciais (acessíveis exclusivamente às partes do processo), de um lado, com versões editadas desses mesmos textos (disponíveis para consulta pública de terceiros), de outro.

Além disso, outras medidas complementares de pseudonimização foram apresentadas pelo Conselho Nacional de Justiça, através dos estudos realizados pelo Comitê de Apoio para Elaboração de Estudos e Pareceres Técnicos sobre a Sistematização do Serviço de Jurisprudência no Poder Judiciário[161], e que são de grande valia para a diminuição da exposição dos dados pessoais e danos dela decorrentes, como: revisar os procedimentos internos relacionados à identificação de casos de segredo de justiça e à implementação dos efeitos decorrentes do acionamento do instituto, a fim de garantir a efetiva proteção de dados pessoais; configurar os sistemas de modo que processos de determinadas classes, assuntos e pelos critérios apresentados neste trabalho sejam considerados em segredo de justiça automaticamente (art. 28, § 3º, da Resolução CNJ nº n. 185, de 2013, do Conselho Nacional de Justiça); considerar, com fundamento no art. 5º da Resolução nº n. 121, de 2010, do Conselho Nacional de Justiça, as opções de suprimir de todos os registros os bancos de jurisprudência os dados estruturados de identificação de partes e advogados(as), aplicar-lhes técnicas de pseudonimização (como o registro apenas das letras iniciais dos nomes) quando relacionados a pessoas naturais e deixar de indexá-los apenas para fins de busca; e considerar as alternativas de abolir dos textos judiciais os cabeçalhos de identificação de partes e advogados ou aplicar-lhes técnicas de pseudonimização (como o registro apenas das letras iniciais dos nomes) relativamente aos dados de pessoas naturais.

[161] CONSELHO NACIONAL DE JUSTIÇA. Tratamento de dados pessoais na consulta de jurisprudência: desafio e perspectivas. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2022/02/tratamento-dados-pessoais-consulta-jurisprudencia30-11-21.pdf. Acesso em: 29 nov. 2022.

Destaca-se que uma parcela dos doutrinadores defendem que não se revela juridicamente admissível a pseudonomização automática e generalizada de dados pessoais contidos em decisões judiciais já publicizadas, por entenderem que no sistema judicial brasileiro o afastamento da regra da publicidade dos atos processuais se submete à reserva de jurisdição, cabendo, portanto, aos(às) magistrados(as) e exclusivamente a eles(as), diante das circunstâncias particulares de cada caso concreto, realizar o juízo de necessidade sobre a publicização de dados pessoais. Porém, no presente trabalho, é possível chegar à conclusão que esse entendimento não deve prevalecer, pois não cabe ao magistrado ter essa autonomia em avaliar e determinar qual dado pessoal deve ser ou não protegido por um dos métodos mencionados, pois as normas da LGPD, demais normas infraconstitucionais e a própria Constituição Federal, no inciso LXXIX do artigo 5º, garantem proteção a todo e qualquer dado pessoal. Logo, todo dado pessoal deve ser protegido conforme a Carta Magna, e, por isso, uma vez que a CF e demais normas infraconstitucionais não especificaram quais dados pessoais merecem ou não proteção, não cabe ao magistrado fazer essa avaliação. Logo, o mais correto a se fazer para que os tribunais possam alcançar a efetividade das normas da LGPD e garantir proteção aos direitos fundamentais da intimidade e privacidade é desenvolver e aplicar métodos de proteção a todos os dados pessoais, sem distinção.

Por fim, além das técnicas de pseudonimização, foi apresentado o método da Autodeterminação Informativa do titular do dado na instituição do segredo de justiça a seus dados pessoais, que seria o próprio titular do dado pessoal, através do advogado ou outro membro do judiciário que o defenda, ter a possibilidade de controle dos seus próprios dados dentro do sistema de um processo judicial eletrônico, sendo permitido selecionar a opção de “Segredo de Justiça - Dado Pessoal - LGPD” para cada protocolo de petição e/ou juntada de documentos que contenham dados pessoais, ou então, por meio de edição daquele dado ou documento pessoal já disponível ou publicizado para que fique em segredo de justiça. Com a aplicação desse método, qualquer dado ou documento pessoal presente em um processo judicial, que não esteja já em segredo de justiça, permanecerá em sigilo de forma automática, apenas acessível às partes, advogados e magistrados vinculados diretamente ao processo judicial. Destaca-se que o método não ferirá o direito fundamental à publicidade dos atos processuais, pois nos processos em que não estiverem em segredo de justiça, o acesso a todos os atos processuais estarão disponíveis, sem restrição, permanecendo apenas os dados e documentos pessoais da parte em sigilo.

Assim, as consequências da aplicação do método da Autodeterminação Informativa pelo titular do dado para instituir de forma autônoma e automática a proteção de seus dados pessoais pelo instituto do segredo de justiça em um processo judicial serão: o magistrado perder a autonomia de decidir quais dados pessoais que integram a privacidade e intimidade das partes devem ser ou não protegidos pelo instituto de segredo de justiça; fazer com que apenas as partes, os advogados e magistrados vinculados ao processo tenham acesso a esses dados pessoais; garantir ao Judiciário mais efetividade às normas da LGPD e respeito aos direitos fundamentais da intimidade e privacidade dos cidadãos.

Portanto, diante de todo o exposto, é possível concluir com o presente estudo que o Poder Judiciário possui legitimidade e dever de aplicar as normas da Lei Geral de Proteção de Dados e que os dados pessoais coletados e armazenados nos sistemas dos Tribunais devem ser regulados conforme as regras de tratamento de dados previstas na lei. Contudo, o tratamento de dados pessoais realizado pelo Poder Judiciário não está totalmente de acordo com as normas da LGPD, pois ainda não estão sendo aplicadas medidas eficazes de proteção aos milhões de dados pessoais expostos dos cidadãos nos processos judiciais eletrônicos, decisões judiciais, jurisprudência e demais serviços de divulgação.

Por isso, as medidas e métodos propostos no trabalho são de grande valia para uma maior efetividade na proteção desses dados, devendo ser aplicados em conjunto, uma vez que apresentam potencial de reduzir consideravelmente o risco de exposição indevida de dados pessoais, garantindo maior efetividade às normas da Lei Geral de Proteção de Dados e respeitando os direitos e princípios fundamentais da Dignidade da Pessoa Humana, como a privacidade e intimidade dos cidadãos. Trata-se de importantes pequenos passos de uma longa caminhada que está apenas começando.

REFERÊNCIAS

AGRA, Walber de Moura. *Curso de direito constitucional*. Belo Horizonte: Editora Fórum, 2018. p. 437.

ALEXY, Robert. *Teoria dos direitos fundamentais*. Trad. Virgílio Afonso da Silva. 2. ed. São Paulo: Malheiros, 2017.

ALVES, Paulo. Ataque hacker ao STJ: seis coisas que você precisa saber sobre o caso. *TechTudo*, [s. l.], 7 nov. 2020. Disponível em: https://www.techtudo.com.br/listas/2020/11/ataque-hacker-ao-stj-seis-coisas-que-voce-precisa-saber-sobre-o-caso.ghtml. Acesso em: 16 jun. 2022.

ARAÚJO, Eugênio Rosa de. Uma introdução aos direitos fundamentais. *Revista da SJR*, Rio de Janeiro, n. 25, p. 315-352, 2009. Disponível em: https://www.jfrj.jus.br/sites/default/files/revista-sjrj/arquivo/17-341-2-pb.pdf. Acesso em: 16 jun. 2022.

BARACHO, José Alfredo de Oliveira. *Direito Processual Constitucional*: aspectos contemporâneos. Belo Horizonte: Fórum, 2006. p. 108.

BARROSO, Luís Roberto. *Curso de Direito Constitucional Contemporâneo*: os conceitos fundamentais e a construção do novo modelo. São Paulo: Saraiva, 2009. p. 192.

BATAGLIA, Murilo Borsio; LEMOS, Amanda Nunes Lopes Espineira; FARRANHA, Ana Claudia. Proteção de Dados Pessoais e Acesso à Informação: Interfaces do Papel da Sociedade Civil no Processo Legislativo Brasileiro. In: XIX Encontro da ANPAD – EnANANPAD 2020. 14 a 16 de outubro de 2020. Disponível em: http://www.anpad.org.br/abrir_pdf.php?e=Mjg5NDA=. Acesso em: 27 nov. 2021.

BESSA, Leonardo Roscoe. *O consumidor e os limites dos bancos de dados de proteção ao crédito*. São Paulo: Editora Revista dos Tribunais, 2003.

BIONI, Bruno Ricardo. *Proteção de Dados Pessoais*: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021.

BIONI, Bruno; DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otávio Luiz Rodrigues. *Tratado de Proteção de Dados Pessoais*. São Paulo: Editora Forense, 2021. p. 139.

BRASIL. *Constituição da República Federativa do Brasil*. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 05 set. 2022.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. *Regula o acesso a informações previsto no inciso XXXIII do art. 5º*, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, DF: Presidência da República, [2011]. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2011- 2014/2011/lei/l12527.htm. Acesso em: 23 ago. 2021.

BRASIL. *Lei n. 12.414, de 9 de junho de 2011*. Brasília, 2011. Disponível em: https://www2.camara.leg.br/legin/fed/lei/2011/lei-12414-9-junho-2011-610758 publicacaooriginal-132782-pl.html. Acesso em: 05 nov. 2021.

BRASIL. *Lei n. 12.965, de 23 de abril de 2014*. Ministério de Ciência, Tecnologia e Inovações, Brasília, 2014. Disponível em: https://antigo.mctic.gov.br/mctic/opencms/legislacao/leis/migracao/Lei_n_12965_de_23 042014__Marco_Civil_da_Internet.html. Acesso em: 12 jan. 2021.

BRASIL. Decreto nº 8.771, de 11 de maio de 2016. *Regulamenta a Lei nº 12.965, de 23 de abril de 2014*, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Brasília, DF: Presidência da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm. Acesso em: 23 ago. 2021.

BRASIL. *Projeto de lei da Câmara n. 5.276, de 2016*. Brasília: Câmara dos Deputados, 2016. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378. Acesso em: 12 jan. 2021.

BRASIL. *Lei n. 13.709, de 14 de agosto de 2018*. Diário Oficial da União, Brasília, 2018. Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/36849373/do1-2018-08-15-lei-no-13-709-de-14-de-agosto-de-2018-36849337. Acesso em: 12 abr. 2020.

BRASIL. *Projeto de lei da Câmara n. 53, de 2018.* Brasília: Câmara dos Deputados, 2018. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/133486. Acesso em: 12 jan. 2021.

BRASIL. Medida Provisória nº 869, de 27 de dezembro de 2018. *Altera a Lei nº 13.709, de 14 de agosto de 2018*, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869.htm. Acesso em: 21 ago. 2021.

BRASIL. Lei nº 13.853, de 8 de julho de 2019. *Altera a Lei nº 13.709, de 14 de agosto de 2018*, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF: Presidência da República, [2019]. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm. Acesso em: 21 ago. 2021.

BRASIL. *Guia de boas práticas*: Lei Geral de Proteção de Dados (LGPD). Brasília, DF: Comitê Central de Governança de Dados, 2021. Disponível em:

https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaLGPD.pdf. Acesso em: 16 jun. 2022.

CANADÁ. *Personal Information Protection and Electronic Documents Act*. Disponível em: https://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html. Acesso em: 01 set. 2022.

CATALA, Pierre. Ebauche d'une théorie juridique de l'information, 2021. p. 20. *In*: DONEDA, Danilo. Da privacidade à proteção de dados: elementos da formação da lei geral de proteção de dados. E-book. 2021. COMMONWEALTH CONSOLIDATED ACTS. 2021. Disponível em: http://www6.austlii.edu.au/cgi-bin/viewdb/au/legis/cth/consol_act/pa1988108/. Acesso em: 01 set. 2022.

CONSELHO NACIONAL DE JUSTIÇA. *Justiça em Números 2022*: Judiciário julgou 26,9 milhões de processos em 2021. Disponível em https://www.cnj.jus.br/justica-em-numeros-2022-judiciario-julgou-269-milhoes-de-processos-em-2021/#:~:text=Justi%C3%A7a%20em%20N%C3%BAmeros%202022%3A%20Judici%C3%A1rio,processos%20em%202021%20%2D%20Portal%20CNJ&text=O%20Poder%20Judici%C3%A1rio%20concluiu%2026,solucionados%20em%20rela%C3%A7%C3%A3o%20a%202020. Acesso em: 21 nov. 2022.

CONSELHO NACIONAL DE JUSTIÇA. *Portaria nº 212 de 15/10/2020*. Institui Grupo de Trabalho destinado à elaboração de estudos e de propostas votadas à adequação dos tribunais à Lei Geral de Proteção de Dados e dá outras providências. Brasília, DF: CNJ, 2020. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3520. Acesso em: 16 jun. 2022.

CONSELHO NACIONAL DE JUSTIÇA. *Portaria nº 63 de 26/04/2019*. Institui Grupo de Trabalho destinado à elaboração de estudos e propostas voltadas à política de acesso às bases de dados processuais dos tribunais e dá outras providências. Brasília, DF: CNJ, 2019. Disponível em: https://atos.cnj.jus.br/atos/detalhar/2890. Acesso em: 16 jun. 2022.

CONSELHO NACIONAL DE JUSTIÇA. *Recomendação nº 73, de 20/08/2020*. Recomenda aos órgãos do Poder Judiciário brasileiro a adoção de medidas preparatórias e ações iniciais para adequação às disposições contidas na Lei Geral de Proteção de Dados – LGPD. Brasília, DF: CNJ, 2020. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3432. Acesso em: 16 jun. 2022.

CONSELHO NACIONAL DE JUSTIÇA. *Resolução nº 363 de 12/01/2021*. Estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais. Brasília, DF: CNJ, 2021. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3668. Acesso em: 16 jun. 2022.

CONSELHO NACIONAL DE JUSTIÇA. *Tratamento de dados pessoais na consulta de jurisprudência: desafio e perspectivas*. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2022/02/tratamento-dados-pessoais-consulta-jurisprudencia30-11-21.pdf. Acesso em 29 nov. 2022.

CONSELHO NACIONAL DE JUSTIÇA. *Tratamento de dados pessoais na consulta de jurisprudência: desafio e perspectivas*. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2022/02/tratamento-dados-pessoais-consulta-jurisprudencia30-11-21.pdf. Acesso em 29 nov. 2022.

CUEVAS, Ricardo Villas Bôas. A incidência da Lei Geral de Proteção de Dados Pessoais nas atividades do Poder Judiciário. *In*: CUEVA, Ricardo Villas Bôas; DONEDA, Danilo; MENDES, Laura Schertel (coord.). *Lei Geral de Proteção de Dados* (Lei n.º 13.709/2018): a caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020. E-book. Disponível em: https:// proview.thomsonreuters.com. Acesso em: 14 out. 2021.

CUEVAS, Ricardo Villas Boas. Anonimização e Pseudonimização de Dados Pessoais no Processo Eletrônico. *In*: TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. *O Direito Civil na era da Inteligência*. São Paulo: Thomson Reuters Brasil, 2020.

DATA PRIVACY BRASIL. *Privacidade e proteção de dados no Congresso Nacional*. Disponível em: https://www.observatorioprivacidade.com.br/projetos-em-numeros/. Acesso em: 21 ago. 2021.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2. ed. Rio de Janeiro: Revista dos Tribunais, 2019. p. 304.

DONEDA, Danilo. Da privacidade à proteção de dados: elementos da formação da lei geral de proteção de dados. E-book. 2021. *In*: DONEDA, Danilo et al.(org.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021.

FALCÃO, Márcio; VIVAS, Fernanda. Supremo investiga suposto ataque hacker a sistema da Corte. *G1*, Brasília, 7 maio 2021. Disponível em: https://g1.globo.com/politica/noticia/2021/05/07/supremo-investiga-tentativa-de-ataque-hacker-a-sistema-da-corte.ghtml. Acesso em: 16 jun. 2022.

FEIGELSON, Bruno; SIQUEIRA, Antonio. *Comentários à Lei Geral de Proteção de dados.* São Paulo: Thompson Reuters Brasil, 2019. p. 43-44.

FRANÇA. *Loi nº 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice*. Paris: Légifrance, 2019. Disponível em: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000038261631/. Acesso em: 16 jun. 2022.

FRANCOSKI, Denise; TASSO, Fernando. Capítulo 14. O Compartilhamento de Dados Pessoais Oriundos de Bases de Dados Públicas: A Compatibilidade Entre a LAI e a LGPD. *In*: FRANCOSKI, Denise; TASSO, Fernando. *A Lei Geral de Proteção de Dados Pessoais*: Lgpd - Ed. 2021. São Paulo (SP): Editora Revista dos Tribunais, 2021. Disponível em: https://thomsonreuters.jusbrasil.com.br/doutrina/1279975732/a-lei-geral-de-protecao-de-dados-pessoais-lgpd-ed-2021. Acesso em: 05 set. 2022.

FRASÃO, Ana. Big Data e Aspectos Concorrenciais do Tratamento de Dados Pessoais. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (coord.). *Tratado de Proteção de Dados*. Rio de Janeiro: Forense, 2021.

GONÇALVES, Diego; RODRIGUES, Bruno Aloy. Os desafios à preservação da intimidade e da privacidade no âmbito virtual: um debate à luz das teorias dos círculos

concêntricos e do mosaico. In: SEMINÁRIO INTERNACIONAL DEMANDAS SOCIAIS; MOSTRA INTERNACIONAL DE TRABALHOS CIENTÍFICOS, 11., 2018, [S. l.]. *Anais* [...]. [S. l.]: UNISC, 2018. Disponível em: https://online.unisc.br/acadnet/anais/index.php/sidspp/article/view/18778/119261205. Acesso em: 16 jun. 2021.

LGPD BRASIL. Novo módulo de consulta pública do Sei deve iniciar a partir de Abril. Disponível em: https://www.lgpdbrasil.com.br/novo-modulo-de-consulta-publica-do-sei-deve-iniciar-a-partir-de-abril/. Acesso em: 06. dez. 2022.

LIMA, Jose Jeronimo Nogueira de. *LGPD e administração pública*: regulação e aplicação' 26/01/2021 147 f. Dissertação (Mestrado em Direito) - Pontifícia Universidade Católica de São Paulo, São Paulo Biblioteca Depositária: PUC/SP, São Paulo, 2021.

MARANHÃO, Juliano de Souza Albuquerque (coord.). Acesso a dados de processos judiciais no Brasil. São Paulo: Associação Lawgorithm de Pesquisa em Inteligência Artificial, [2020]. Disponível em: https://lawgorithm.com.br/wp-content/uploads/2020/07/ReportAcessoDadosJudiciário.pdf. Acesso em: 16 jun. 2022.

MENDES, Laura Schertel. *Transparência e privacidade*: violação e proteção da informação pessoal na sociedade de consumo. 2008. 17 f. Dissertação (Mestrado em Direito) - Universidade de Brasília, Brasília, 2008.

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Editora Saraiva Jur, 2017.

MENKE, Fabiano; GOULART, Guilherme Damasio. Segurança da Informação e Vazamento de Dados. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (coord.). *Tratado de Proteção de Dados*. Rio de Janeiro: Forense, 2021.

METRÓPOLES. *Após ataque hacker, site do TJDFT segue fora do ar pelo 3º dia seguido*. Disponível em: https://www.metropoles.com/distrito-federal/apos-ataque-hacker-site-do-tjdft-segue-fora-do-ar-pelo-3o-dia-seguido. Acesso em: 21 nov. 2022.

MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais. *Revista do Advogado*, n. 144, p. 50, nov. 2019.

NAÇÕES UNIDAS BRASIL. *Os Objetivos de Desenvolvimento Sustentável no Brasil*. Disponível em: https://nacoesunidas.org/direitoshumanos/declaracao/. Acesso em: 01 set. 2022.

NUNES, Natália Martins. *O tratamento irregular de dados pessoais e o dever de reparar os danos causados*. 2018. Disponível em: https://ndmadvogados.com.br/artigos/o-tratamento-irregular-de-dados-pessoais-e-o-dever-de-reparar-os-danos-causados. Acesso em: 21 set. 2021.

OLIVEIRA, Frank Ned Santa Cruz de. Gestão de riscos no direito fundamental à privacidade de dados pessoais no Processo Judicial Eletrônico / Diário de Justiça Eletrônico. 2020. 136 f., il. Dissertação (Mestrado Profissional em Computação Aplicada) - Universidade de Brasília, Brasília, 2020.

OLIVEIRA, Caio César de. A Autoridade Nacional de Proteção de Dados (ANPD) e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. *In*: MULHOLLAND, Caitlin (coord.). *A LGPD e o novo marco normativo do Brasil*. Porto Alegre: Arquipélago, 2020. p. 380-383.

ORDEM DOS ADVOGADOS DO BRASIL. Brasil tem 1 advogado a cada 164 habitantes; CFOAB se preocupa com qualidade dos cursos jurídicos. 2022. Disponível em: https://www.oab.org.br/noticia/59992/brasil-tem-1-advogado-a-cada-164-habitantes-cfoab-se-preocupa-com-qualidade-dos-cursos-juridicos. Acesso em: 25 nov. 2022.

ORTIZ, Brenda. Por suspeita de ataque hacker, TRF-1 retira do ar portal da Justiça Federal do DF e de 13 estados. *G1*, Brasília, 27 nov. 2020. Disponível em: https://g1.globo.com/df/distrito-federal/noticia/2020/11/27/por-suspeita-de-ataque-hacker-trf-1-retira-do-ar-portal-da-justica-federal-do-df-e-de-13-estados.ghtml. Acesso em: 12 set. 2021.

PADILHA, Rodrigo. *Direito Constitucional*. 5. ed. rev. ampl. Rio de Janeiro: Forense, São Paulo: Método, 2018. p. 805.

PELLEGRINO, Maria Cristina Conde. *DA MIHI DATA, DABO TIBI JUS*: o tratamento de dados pessoais no âmbito do processo judicial eletrônico brasileiro, à luz da Lei Geral de Proteção de Dados' 13/07/2021 147 f. Dissertação (Mestrado em Instituições Sociais, Direito e Democracia) - Universidade FUMEC, Belo Horizonte Biblioteca Depositária: FCH, Belo Horizonte, Minas Gerais, 2021.

PINHEIRO, Patrícia Peck. *Proteção de Dados Pessoais*: comentários à Lei n. 13.709/2018 LGPD. São Paulo: Editora Saraiva, 2018.

POLÍCIA CIVIL inicia investigação sobre ataque cibernético ao sistema do TJ-RS. G1, [s. l.], 30 abr. 2021. Disponível em: https://g1.globo.com/rs/rio-grande-do-sul/noticia/2021/04/30/policia-civil-inicia-investigacao-sobre-ataque-ao-sistema-informatico-do-tj-rs.ghtml. Acesso em: 16 jun. 2022.

REALE, Miguel. *Lições preliminares de direito*. 25. ed. São Paulo: Saraiva, 2001. p. 87-88.

RIO GRANDE DO SUL. Tribunal de Justiça do Estado do Rio Grande do Sul. *Nota de esclarecimento*. Porto Alegre: TJRS, 11 nov. 2020. Disponível em: https://www.tjrs.jus.br/novo/noticia/nota-de-esclarecimento-3/. Acesso em: 16 jun. 2022.

RODOTÁ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SARLET, Ingo Wolfgang. A EC 115/22 e a proteção de dados pessoais como Direito Fundamental I. *Revista Consultor Jurídico*, 2022. Disponível em: https://www.conjur.com.br/2022-mar-11/direitos-fundamentais-ec-11522-protecao-dados-pessoais-direito-fundamental. Acesso em: 14 set. 2022.

SISTEMA de processos do TJ-RS sofre ataque hacker nesta quarta-feira. *Revista Consultor Jurídico*, [s. l.], 11 nov. 2020. Disponível em:

https://www.conjur.com.br/2020-nov-11/sistema-eproc-tj-rs-sofre-ataque-hacker-nesta-quarta-feira. Acesso em: 16 jun. 2022.

SOMBRA, Thiago Luís Santos. Fundamentos da regulação da privacidade e proteção de dados pessoais: pluralismo jurídico e transparência em perspectiva. *Revista dos Tribunais*, 2019.

STF. MC ADI: 6388 DF - DISTRITO FEDERAL 0090568-75.2020.1.00.0000, Relator: Min. ROSA WEBER, Data de Julgamento: 17/04/2020, Data de Publicação: DJe-102 28/04/2020.

TASSO, Fernando Antonio; MALDONADO, Viviane N. Brega; BLUM, Renato Opice (coord.). *LGPD*: Lei Geral de Proteção de Dados. São Paulo: Revista dos Tribunais, 2019. p. 252.

TECMASTERS. Senado aprova MP que dá autonomia à Autoridade de Proteção de Dados. Disponível em: https://tecmasters.com.br/senado-mp-autonomia-autoridade-protecao-dados/. Acesso em: 11 dez. 2022.

TORCHIA, Bruno Martins; MACHADO, Tacianny Mayara Silva. A reponsabilidade subjetiva prevista ne lei geral de proteção de dados e a relação jurídica centre controlador e o encarregado de proteção de dados. *In*: DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes (coords.). *LGPD & Administração Pública*. São Paulo: Thomson Reuters Brasil, 2020. p. 833.

TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E TERRITÓRIOS. Aqui tem PjE. Disponível em: https://www.tjdft.jus.br/pje/aqui-tem-pje. Acesso em: 9 dez. 2022.

UNIÃO EUROPEIA. *Convenção Europeia dos Direitos dos Homens*. Disponível em: https://www.echr.coe.int/Documents/Convention_POR.pdf. Acesso em: 01 set. 2022.

UNIÃO EUROPEIA. *Council of Europe*. 1981. Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37. Acesso em: 01 set. 2022.

UNIÃO EUROPEIA. *Directiva 95/46/CE do Parlamento Europeu e do Conselho*. 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 01 set. 2022.

UNIÃO EUROPEIA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016*. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679. Acesso em: 01 set. 2022.

UNIÃO EUROPEIA. *Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016*, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). [S. l.]: EUR-Lex, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 16 jun. 2022.

UNIVERSIDADE FEDERAL DO PARANÁ. Ferramenta do SEI! vai ajudar na proteção de dados: veja como usar. 2021. Acessível em:

https://www.ufpr.br/portalufpr/noticias/ferramenta-do-sei-vai-ajudar-na-protecao-de-dados-pessoais-veja-como-usar/. Acesso em: 06. dez. 2022.

ZARDO, Francisco. As sanções administrativas de multa simples e multa diária na LGPD. *In*: DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes (coords.). *LGPD & Administração Pública*. São Paulo: Thomson Reuters Brasil, 2020. p. 701.