13

PROTEÇÃO DOS DADOS PESSOAIS E PROCESSO JUDICIAL ELETRÔNICO: COMO HARMONIZAR JUSTIÇA ABERTA E AUTODETERMINAÇÃO INFORMACIONAL?

PROTECTION OF PERSONAL DATA AND ELETCRONIC JUDICIAL PROCESS: HOW TO HARMONIZE OPEN JUSTICE AND INFORMATIONAL SELF-DETERMINATION?

Recebido: 22/03/2024
Aceito: 06/06/2024

José Marcos Lunardelli
Professor do Mestrado Profissional da ENFAM
Doutor e Mestre em Direito Econômico - USP
Desembargador Federal do TRF3

RESUMO: O presente artigo analisa a Lei Geral de Proteção de Dados – LGPD – Lei 13.709/2018 – e a transformação digital do Poder Judiciário com a adoção do Processo Judicial Eletrônico, bem como a necessidade de repensar o modelo de ampla publicidade processual e de dados abertos ao público, com a sua compatibilidade com a autodeterminação informacional garantida pelas normas de proteção dos dados pessoais da LGPD.

PALAVRAS-CHAVE: Proteção de Dados – Privacidade -Autodeterminação Informacional - Publicidade Processual – Processo Judicial Eletrônico – Lei 13.709/2018.

ABSTRACT: *This article examines the General Law on Protection of Personal Data (LGPD) - Law No. 13.709/2018 - and the digital transformation of the Judiciary System with the Electronic Law Process, as well as the need to rethink the model of broad process publicity and open data to the public, with its*

compatibility with informational self-determination guaranteed by personal data protection norms of the LGPD.

KEYWORDS: Data protection – Privacy – Informational self-determination – Process publicity - Electronic legal process – Law No. 13.709/2018

INTRODUÇÃO

A sociedade informacional é resultado da revolução provocada pelas inovações no campo da microeletrônica, da computação e das comunicações, que aumentaram exponencialmente a capacidade de processamento de dados ao desmaterializar as formas tradicionais de registro das informações, convertendo-as no formato binário (*bytes*).

Os diversos artefatos eletrônicos e comunicacionais, utilizados nas interações sociais e econômicas, encontram-se tão profundamente integrados na nossa vida que se tornaram praticamente invisíveis, borrando as fronteiras do *on-line* e *off-line*, devido à sua onipresença no dia a dia das pessoas, além de serem o mecanismo central de monitoramento das ações e reações dos indivíduos no mundo digital informacional.

Na sociedade agrícola, a terra era insumo fundamental; na industrial, o carvão e a eletricidade; na era informacional, o vetor de propulsão do mercado são os dados pessoais coletados, principalmente no mundo interconectado da Internet[1]. Tais dados são capturados intensamente nos modelos de negócios baseados na oferta de serviços que aparentemente são "gratuitos", mas, na verdade, revelam-se onerosos, pois sempre demandam em troca deles a cessão de informações dos usuários, as quais são coletadas, armazenadas e, muitas vezes, transferidas a terceiros.[2]

Essa é a moeda de troca do mundo digital suspostamente gracioso que confirma a expectativa de que, nas relações de mercado, não existe almoço grátis. Sempre haveria um *trade off*, ainda que não explícito, pelos agentes econômicos.

1 Castells (2023, p. 124) argumenta que, no atual modelo de organização socioeconômica, "a informação é a sua matéria prima: são tecnologias para agir sobre a informação, não apenas a informação para agir sobre a tecnologia como foi o caso das revoluções tecnológicas anteriores. "

2 Bom exemplo são os *cookies* que servem para a produção de perfis comportamentais e de consumo com base nos dados capturados. De acordo com Palhares (2020, p.13) "cookies podem armazenar diversas informações sobre os hábitos de utilização da internet dos usuários, desde os links em que foram clicados, os produtos que foram comprados, os termos que foram pesquisados, a região em que vive o usuário, e tantos outros dados valiosos para uma eventual segmentação de publicidade, que vão muito além dos objetivos para os quais foram inicialmente concebidos, de meramente viabilizar algumas funcionalidades específicas.".

É no processo de monitoramento permanente e no rastreamento das pegadas digitais das pessoas que transitam pelos domínios da Internet que frequentemente se extrai o novo combustível da economia informacional (dados pessoais), que impulsiona as atividades especializadas em extrair vantagens econômicas da comercialização de perfis comportamentais utilizados para novos formatos de publicidade personalizada, bem como para fins potencialmente negativos, como as classificações, discriminações e também modalidades perigosas de controle social.

Nesse contexto de vigilância e controle inerente à sociedade informacional a tutela jurídica dos dados pessoais se apresenta como primordial para a promoção dos direitos fundamentais de liberdade e igualdade das pessoas.

O Judiciário vive um processo de transformação digital com a substituição do modelo tradicional de compilação das informações nos processos judiciais – justiça de papel – pelo registro em documentos eletrônicos com a implantação do Processo Judicial Eletrônico.

Pretende-se neste ensaio refletir sobre a transformação digital da Justiça e a necessidade de buscar um novo equilíbrio entre o modelo de ampla publicidade e de acesso aos autos dos processos judiciais, que historicamente tem orientado a prestação jurisdicional, com a proteção dos dados pessoais expostos nos sistemas de informações processuais, à vista dos valores e interesses albergados na Lei Geral de Proteção de Dados – (Lei 13.709/2018 - LGPD, doravante), a fim de analisar a necessidade de ponderação entre as normas relativas à publicidade processual e as que protegem os dados pessoais.

Para tal desiderato, este trabalho está organizado da seguinte forma: após essa introdução, na primeira seção, faz-se uma sintética revisão das mutações ocorridas no campo da privacidade com a emergência da proteção de dados como direito fundamental à autodeterminação informativa, analisando precedentes jurisprudenciais do Tribunal Constitucional alemão e do Supremo Tribunal Federal; na segunda, examina-se a racionalidade regulatória da LGPD, bem como a sua aplicabilidade ao Judiciário; na terceira, a transformação digital da Justiça com o Processo Judicial Eletrônico e a busca de harmonização entre a proteção dos dados pessoais e as normas de publicidade processual e encerra-se com algumas considerações finais.

1 DA PRIVACIDADE À PROTEÇÃO DE DADOS

1.1 Mutações no conceito de privacidade

O "direito de ser deixado só" - "*right to be alone*" – ganhou notoriedade, como expressão síntese de certa perspectiva do direito à privacidade, graças à reflexão jurídica de Warren e Brandeis (1890), publicada na Harvard Law Review, na qual, eles sustentaram a tese de que constituiriam atos ilícitos certas práticas midiáticas que invadiam os "recintos sagrados da vida privada e doméstica"[3] (Warren; Brandeis, 1890). Esse artigo seminal repercutiu intensamente na *common law* e alhures[4], pois teve o mérito de inovar ao defender uma concepção de direito à privacidade que não derivava do direito de propriedade, mas sim da inviolabilidade da pessoa.

Tal noção de privacidade guiava-se pela exclusão de olhares indesejáveis da esfera privada, repelindo desse espaço quem não fora convidado a nele ingressar, ressaltando a centralidade do sigilo em certos aspectos da vida privada e da intimidade que não deveriam ser revelados sem o consentimento do titular.

A dimensão de escudo contra intromissões indevidas, espécie de liberdade negativa, seria um forte componente dessa visão subjetiva de privacidade, que facultava a cada indivíduo a prerrogativa de "decidir se aquilo que é seu será dado ao público" (Warren; Brandeis, 1890).

O debate sobre o poder do Estado de coletar e armazenar informações pessoais em banco de dados centralizados, com a justificativa de gerir com mais eficiência os serviços públicos, recolocou o tema da privacidade em ribalta, visto que expunha os cidadãos ao risco de controles autoritários propiciados pela ampliação da capacidade de vigilância estatal proporcionados pelas novas tecnológicas computacionais.

---

3 Conforme explica Zanini (2015, p. 11) não haveria certeza sobre "a motivação de Warren e Brandeis para a publicação do artigo dedicado ao *privacy*. Alguns estudiosos especulam que foi uma resposta ao aumento de sensacionalismo da imprensa em geral. Outros apontam que seria uma reação direta aos abusos cometidos pela imprensa contra a família de Warren, uma das mais influentes na sociedade de Boston do final do século XIX.".

4 Doneda (2006, p. 138-139) relata que esse artigo jurídico é uma referência frequente em trabalhos sobre privacidade e costuma estar entre os mais citados nos Estados Unidos.

São representativos desse debate nos anos 60 e 70 os dilemas e contradições que envolveram a proposta do *National Data Center,* nos EUA[5] e também o projeto SAFARI, na França[6], nos quais se concentrariam dados de identificação dos cidadãos. Os dois projetos não prosperaram, pois devido a temores o uso de tais informações em detrimento da cidadania, além de se entrever riscos ao modelo democrático de Estado em tais empreendimentos, suscitando intensos debates sobre privacidade e direitos individuais.

O desenvolvimento da tecnologia de processamento eletrônico de informações descortinou novos problemas que não eram solucionados no paradigma clássico de privacidade, que se estruturava na lógica da liberdade negativa de exclusão de ingerências externas no campo da vida privada e íntima, pois não contemplava as preocupações com uso abusivo de dados pessoais por agentes públicos ou privados que controlavam bases de dados obscuras e genéricas.

O conceito de privacidade foi redimensionado para conferir maior protagonismo ao cidadão na gestão do fluxo informacional, o qual passou a incorporar a ideia de controle sobre os próprios dados, definindo Westin (1967, p. 7) privacidade como "a reivindicação de indivíduos, grupos ou instituições de determinar por si próprios quando, como e em que medida a informação sobre eles é comunicada a outros".

Rodotà (2008, p, 93) destacou, como significativo dessa mutação no ideal de privacidade, que a sequência mais relevante estaria no trinômio "pessoa-circulação-controle e não mais pessoa-informação-sigilo, em torno da qual foi construída a clássica noção de privacidade", sublinhando, ainda, a importância dessa evolução no conceito de privacidade na construção de uma "cidadania eletrônica"

5 Conforme relata Doneda (2006, p.184-185) "por volta de 1965 o *Bureau of Budget*, responsável pelo orçamento americano apresentou uma proposta, aparentemente simples (...): construir uma central única de armazenamento de informações pessoais (*National Data Center*), reunindo informações sobre os cidadãos norte-americanos disponíveis em outros órgãos da administração federal em um único banco de dados".

6 Também segundo Doneda (2006, p. 190) no início da década de 70 se projetou o "SAFARI – *Système Automatisè pour les Fichiers Administratif et le Répertoire des Individus*, que consistia na transferência dos dados pessoais dos cidadãos franceses nas mãos da administração pública para sistemas informatizados", a fim de que de cada pessoa fosse "identificada por um número – o seu *Sécurité Sociale* – invariável por toda a vida". Em consequência desse debate, emergiu a primeira geração de normas protetivas de dados pessoais com enfoque sobretudo na tecnologia de armazenamento como a Lei do *Land* Alemão Hesse (1970); na Suécia, Estatuto para banco de dados 1973 – *Data Legen* 298; *Privacy Act* americano em 1974 (Doneda, 2006, p. 206-207).

que assegurasse a "indispensável da liberdade existencial" e o controle sobre o uso das próprias informações "em qualquer momento em qualquer lugar" como expressão do 'direito à autodeterminação informativa' segundo a definição introduzida pela Corte Constitucional alemã." (Rodotà, 2008, p. 144).

Essa leitura evolucionista do conceito de privacidade para incorporar a autodeterminação informacional é criticada por Bioni (2021), que defende que o melhor enquadramento dogmático do tema relativo à proteção de dados não seria na concepção revista de privacidade, mas sim como uma "espécie nova no rol dos direitos da personalidade", expandindo, dessa forma, a fronteira desses direitos[7].

Segundo Bioni (2021), a dialética privada *versus* público, na qual se construiu a concepção tradicional de privacidade como liberdade negativa, não dá conta do dinâmico fenômeno da proteção de dados, cujo elemento determinante é o vínculo dos dados à pessoa humana e a necessidade de prevenção e repressão do uso abusivo deles no processo de circulação das informações na sociedade.

1.2 Autodeterminação informacional no Tribunal Constitucional alemão: Lei do Recenseamento

Para amparar o conjunto de situações subjetivas imbricadas no tratamento de dados pessoais, em 1983, o Tribunal Constitucional alemão desenvolveu o conceito de autodeterminação informacional, como direito fundamental autônomo derivado do direito geral de personalidade[8], com base em normas da Lei Fundamental, que asseguravam a "dignidade humana" e o 'livre desenvolvi-

7 Bioni (2021, p. 96) argumenta que: "o direito à proteção de dados deve ser alocado como uma nova espécie do rol aberto dos direitos da personalidade, dando elasticidade à cláusula geral da tutela da pessoa humana. Caso contrário, corre-se o risco de ele não se desprender das amarras conceituais e da dinâmica do direito à privacidade e, em última análise, inviabilizar uma normatização própria para regular o fluxo informacional como fator promocional da pessoa humana.".

8 Consoante explica Mendes (2020, p. 7-9) o Tribunal Constitucional Alemão construiu em diversos casos a jurisprudência relativa ao direito geral de personalidade, como uma norma aberta cuja definição concreta da sua extensão dar-se-ia casuisticamente, prevendo, dessa forma, um direito de liberdade indefinido subsidiário de liberdades específica, o qual protegeria contra os riscos desconhecidos.

mento da personalidade", ao julgar o caso BVerfGE, 61[9] (Volkszählung) (Martins, 2016, p. 55-63).

Com base na premissa de que havia uma modificação das condições técnicas de processamento de dados, com a superação dos métodos manuais (fichas e pastas), o Tribunal concluiu que era essencial um escrutínio mais rigoroso dos critérios de tratamento das informações dos cidadãos, pois o valor intrínseco de um dado pessoal não era mais resultado da sua própria natureza, mas das múltiplas combinações que seriam passíveis de realização com o uso da capacidade computacional disponível, declarando que não havia mais "dados insignificantes" no contexto tecnológico atual.

Em face desse cenário era imprescindível intensificar a transparência do processo de tratamento de informações, mormente na realização do censo para o qual se admitem usos multifuncionais dos dados para fins estatísticos, a fim de garantir "que indivíduo não se torne um simples objeto da informação no contexto de levantamento e manipulação automáticos dos dados relativos à sua pessoa" (Martins, 2016, p. 59).

Os cidadãos deveriam ter efetivo conhecimento e liberdade para "determinar, com suficiente segurança, quais informações sobre a sua pessoa são conhecidas em certas áreas do seu meio social", ressaltando que uma sociedade na qual "os cidadãos não soubessem mais quem, o quê, quando, e em que ocasião se sabe sobre eles não seriam compatíveis com o direito à autodeterminação na informação" (Martins, 2016, p. 58).

Esse direito à autodeterminação informativa não era garantido irrestritamente, pois o indivíduo não teria um domínio absoluto sobre "seus" dados, visto que as necessidades comunicacionais da vida comunitária justificariam "limitações de seu direito à autodeterminação sobre as informações em favor do interesse geral predominante", conforme ressalvado pelo Tribunal (Martins, 2016, p. 58).

9 O Tribunal Constitucional Federal alemão julgou parcialmente inconstitucional a "Lei do Recenseamento de População, Profissão, Moradia e Trabalho" de 25 de março de 1982, proclamando a nulidade de dispositivos legais que facultavam a transferência dos dados pessoais a outros órgãos e também autorizavam a comparação dos dados coletados com outros registros. Destacou-se que, enquanto não anonimizados, esses dados não poderiam ser transferidos a terceiros.

Segundo Mendes (2020 p.10-13), a autodeterminação informacional não teria por objeto a tutela dos dados *per se* mas a pessoa aos quais eles estão vinculados. Nesse novo tipo de proteção não teria mais relevância perquirir qual o âmbito de proteção (privado ou íntimo) que determinado dado poderia ser incluído, pois todos os dados pessoais se encontrariam amparados juridicamente, visto que são projeções da personalidade humana na sociedade, cujo destino o titular tem o direito de decidir.

A autodeterminação informacional, na forma como elaborada pelo Tribunal Constitucional alemão, transcende a ideia clássica de privacidade, porquanto, em vez de uma abordagem concentrada no sigilo e na dicotomia entre o público e o privado, optou-se por dar "atenção aos possíveis efeitos do processamento de informações para autonomia humana" (Schwartz, 1989, p. 676), pois dados aparentemente irrelevantes poderiam assumir novos significados dependendo do contexto, finalidade e modo de tratamento.

1.3 Proteção de dados na jurisprudência do STF: caso IBGE

O STF também teve a oportunidade de reconhecer a proteção de dados como direito fundamental autônomo. Isso se deu quando o Plenário da Suprema Corte, em 06 e 07 de maio de 2020, referendou Medida Cautelar na ADI 6387-DF[10], onde se discutiu a constitucionalidade da Medida Provisória 954/2020 que previa o compartilhamento de dados pessoais dos usuários dos serviços de telecomunicações (telefones fixos - STFC - e celulares – SMP) com o IBGE – Fundação Instituto Brasileiro de Geografia e Estatística (art. 1º - MP 954/2020)[11].

10 Também se julgou conjuntamente as ADIs 6.388, 6389, 6.290 e 6.393 que tinham objetos idênticos.

11 Em síntese, a Medida Provisória 954/2020 determinava que se comunicasse ao IBGE, em meio eletrônico, *a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas* (art. 2º, caput, MP 954/2020). Previa que tais dados seriam utilizados para *produção de estatística oficial, com objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares* (§ 1º, art. 2º, MP 954/2020), durante o período da pandemia da Covid-19. Delegava ao Presidente do IBGE, ouvida a Agência Nacional de Telecomunicações, o estabelecimento do procedimento de disponibilização dos dados, nos prazos estipulados na própria Medida Provisória (§ 2º e 3º, art. 2º MP 954/2020). Estipulava que os dados compartilhados teriam o caráter sigiloso; uso para a finalidade exclusiva de pesquisa estatística e que não seriam utilizados como objeto de certidão ou prova em processo administrativo, fiscal ou judicial, proibindo a transferência dos dados para entidades públicas ou privadas, prevendo ainda a realização de relatório de impacto à proteção e dados pessoais (art. 3º MP 954/2020).

Com um olhar atento para a realidade tecnológica e a importância dos dados pessoais na sociedade informacional, o STF realizou uma interpretação sistemática das normas constitucionais previstas no artigo 1º, III, (dignidade da pessoa humana); art. 5º, X e XII (tutela da privacidade em sentido amplo); art. 5º, LXXII (habeas data como remédio constitucional para acesso e retificação de informações) e depreendeu a existência de um direito fundamental à proteção de dados que tutela a autodeterminação informacional, como também já havia decidido o Tribunal Constitucional alemão no caso da lei do recenseamento.

Apesar de em diversos momentos do julgamento tenha-se sublinhado o papel crucial das estatísticas para a produção de políticas públicas baseadas em evidências e também a seriedade institucional do IBGE, entendeu-se que havia muitas lacunas regulatórias na Medida Provisória 954/2020, não disciplinava de forma clara e precisa o processo de compartilhamento, visto que trazia uma finalidade muito abstrata – o genérico objetivo de produzir estatística oficial - além de não haver uma relação de proporcionalidade entre os dados necessários para pesquisa (dados amostrais) e a transferência total de informações relativa a milhões de usuários dos serviços de telecomunicações, o que atentava contra o princípio da necessidade em matéria de proteção de dados.

Também maculava o processo a existência de um déficit de regulação nos procedimentos de compartilhamento de dados previstos na Medida Provisória 954/2020, que não disciplinava suficientemente as salvaguardas necessárias às informações compartilhadas, além de se prever uma inversão no modo de elaboração do relatório de impacto à proteção de dados que não seria realizado previamente ao tratamento de dados, a fim de identificar riscos e procurar preveni-los ou mitigá-los, como recomendam as boas práticas de governança de dados e a própria LGPD (Lei 13.709/2018), que não se encontrava ainda vigente, mas no período da *vacatio legis*, o que realçava a situação de fragilidade da arquitetura institucional disponível para a supervisão do processo de compartilhamento de informações.

Em diálogo com a decisão do Tribunal Constitucional alemão, que afirmou o direito à autodeterminação informacional (BVerfGE, 61 - Volkszählung), foi lembrado que, no atual estado da arte da tecnologia de processamento de dados,

não existem mais dados pessoais insignificantes, tendo sido rejeitado o argumento de que seriam simples registros cadastrais não sigilosos que, até há pouco tempo, eram objeto de publicação em listas telefônicas. Desde que fossem dados com aptidão para identificação de pessoas, mereceriam tutela jurídica, pois, adequadamente tratados pelos métodos eletrônicos de processamento, poderiam adquirir outro significado e, se fossem mal utilizados, lesariam direitos da personalidade dos indivíduos.

No voto da Ministra Rosa Weber (ADI 6387-MC-REF/DF, p. 10), restou consignado que "tais informações [nome, números de telefones e endereços de seus consumidores, pessoas físicas ou jurídicas] relacionadas à **identificação – efetiva ou potencial – de pessoa natural,** configuram **dados pessoais** e integram, nessa medida, o âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (**art. 5º, *caput***), da privacidade e do livre desenvolvimento da personalidade (**art. 5º, X e XII**). Sua manipulação e tratamento, desse modo, hão de observar, sob pena de lesão a esses direitos, os limites delimitados pela proteção constitucional. "[12]

Essa confirmação do valor jurídico dos dados pessoais significou uma mudança na lógica de proteção de dados na jurisprudência do STF, pois não se debateu o problema com fundamento no seu enquadramento em alguma categoria especial que justificasse qualquer tipo de sigilo (dados privados ou íntimos), mas com base nos riscos que os usos inadequados de informações pessoais poderiam acarretar aos direitos fundamentais de liberdade, da privacidade e da personalidade.

O reconhecimento do *status* constitucional do direito à proteção de dados por força da compreensão integrada de normas constitucionais pelo STF reper-

12 Ao analisar essa decisão, Mendes (2021, p. 65) anota que "representa uma evolução em relação à jurisprudência anterior do STF", pois "a interpretação conferida foi a de que qualquer dado que leve à identificação de uma pessoa pode ser usado para a formação de perfis informacionais de grande valia para o mercado e o Estado e, portanto, merece proteção constitucional. Nesse sentido, tem-se maior flexibilidade e abertura dessa tutela constitucional, podendo-se aplicar tal direito fundamental a uma multiplicidade de casos envolvendo a coleta, o processamento ou a transmissão de dados pessoais, em razão de não se ter um conteúdo fixo de garantia, nem limitá-lo apenas às informações pertencentes à esfera privada.

cutiu no próprio legislador constitucional, que emendou o catálogo de direitos fundamentais para incluí-lo no art. 5º, LXXIX, ao prescrever que: "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais" (Emenda Constitucional 115/22).

É indiscutível a autonomia do direito à proteção de dados, cujo objeto de tutela é o dado pessoal de pessoa identificada ou identificável, que pode ser utilizado em alguma espécie de tratamento e, por isso, comporta o risco da má-utilização e danos à personalidade. Como Sublinha Queiroz (2019, p. 19) "ao contrário do direito à privacidade, o direito à proteção de dados não faz, em princípio, um filtro substantivo sobre a qualidade do dado para decidir se ele está ou não em seu escopo: se é dado pessoal, interessa ao direito da proteção de dados pessoais, ainda que não seja sensível à privacidade do titular.".

1.4 Proteção de dados e a sua dimensão coletiva

Novas estratégias regulatórias foram desenvolvidas, quando se constatou a debilidade do consentimento como ferramenta central para o exercício da autodeterminação informacional, à vista das limitações cognitivas dos indivíduos e também das relações assimétricas de poder existentes na sociedade informacional[13].

A proteção de dados pessoais não poderia ser concebida tão somente com apoio na perspectiva individualista ou patrimonialista da problemática, mas sim dentro da sua dimensão coletiva, na qual se expressam, segundo Doneda (2006, p. 144), "complexos interesses, tanto do titular quanto da coletividade que pode dar origem a poderes bem como a deveres, obrigações, ônus aos envolvidos", que deveriam regular processualmente o fluxo controlado das informações.

Essa tutela dinâmica acompanharia os dados pessoais em toda a sua trajetória, pois a autodeterminação informacional não se exauria na autogestão do

13 Refletindo sobre os altos custos sociais e econômicos inerentes ao exercício consciente do consentimento, os quais muitas vezes poderiam excluir as pessoas do acesso a bens e serviços, Doneda (2006, p.212) sublinha que "a autodeterminação informativa, portanto, continuava sendo o privilégio de uma minoria que decidia enfrentar tais custos".

consentimento[14], exigindo, dessa forma, um arcabouço regulatório mais efetivo que governasse o tratamento de dados em múltiplos espaços (públicos e privados), tendo em vista o valor social dos dados pessoais.

Era necessária uma infraestrutura institucional e legal que contemplasse os múltiplos riscos inerentes à circulação de dados pessoais, os quais repercutem na projeção social e relacional do indivíduo na sociedade cada vez mais digitalizada, podendo afetar a sua identidade e, por conseguinte, o livre desenvolvimento da personalidade.

É nesse âmbito de disciplina holística dos dados pessoais como um bem comum que se insere a LGPD[15]. Na próxima seção, analisar-se-á este estatuto normativo[16], a fim de examinar alguns institutos que se relacionam com a transformação digital do Judiciário, bem como seu o impacto na publicidade das informações processuais.

2 PROTEÇÃO DE DADOS NA LGPD

2.1 Racionalidade regulatória

A Lei 13.709/2018 (LGPD) disciplinou a proteção de dados de maneira horizontal, abrangendo todos os atores (pessoas naturais ou pessoas jurídicas de

14 Para uma crítica à sobrecarga posta sobre o consentimento individual como mecanismo central para autogestão do processo de proteção de dados, ver Solove (2013).

15 Mesmo antes do advento da LGPD, os dados pessoais eram objetos de normatização setorial em questões específicas do ordenamento jurídico. Em âmbito constitucional, havia preceitos relativos ao direito à vida privada e à vida íntima (art. 5º, X) e ao sigilo das comunicações (art. 5º, XII) ao habeas data que tinha por escopo garantir o acesso às informações e a possibilidade de retificações de incorreções. No plano infraconstitucional, o Código de Defesa do Consumidor (Lei 8.078/90) também trouxe normas sobre o cadastro de consumidores (acesso, comunicação, correção e delimitação temporal); a Lei do Cadastro Positivo (Lei 12.414/2011) viabilizou um microssistema de tratamento de dados de adimplementos para a constituição de perfis de créditos; a Lei de Acesso às Informações (Lei 12.527/11) assegurou maior transparência da administração pública; o Marco Civil da Internet (Lei 12.965/2014) que também se preocupou com a privacidade e a proteção de dados dos usuários da Internet, ainda que maneira tópica. Em todos esses diplomas normativos especiais, o tema era regulado de forma fragmentada e restrita, carecendo de organicidade e coerência, o que gerava muita insegurança jurídica. O desafio hermenêutico hodierno é buscar o diálogo e complementaridade entre essas regulações especiais e a LGPD.

16 Não se faz uma análise exauriente desse microssistema normativo, o que estaria fora do escopo desse trabalho, mas tão somente de determinados temas que explicitam a racionalidade regulatória dos dados pessoais na LGPD.

direito público ou privado)[17] envolvidos no processo de tratamento[18] de dados pessoais, fixando direitos, deveres e ônus de cada um, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Com base nos pressupostos de que, na sociedade informacional, não há dados pessoais irrelevantes e que o tratamento deles constitui atividade de risco à representação da pessoa na sociedade, a LGPD estruturou um modelo de regulação *ex ante* para proteção de dados pessoais, visando à segurança jurídica e à regulamentação do fluxo informacional em todo o seu ciclo (da coleta à eliminação), fixando os direitos e obrigações dos diversos atores públicos e privados que interagem, direta ou indiretamente, no processo de tráfico de dados.

O regime jurídico das informações pessoais tem por alicerce valores ancorados em normas constitucionais, que devem orientar a interpretação e aplicação harmônica dos institutos da LGPD, tais como: i. respeito à privacidade; ii. autodeterminação informativa; iii. liberdade de expressão, de informação, de comunicação e de opinião; iv. inviolabilidade da intimidade, da honra, e da imagem; v. desenvolvimento econômico e tecnológico e a inovação; livre iniciativa, livre concorrência e a defesa do consumidor; vi. os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Para que haja conformidade ao modelo previamente desenhado pelo legislador, o tratamento de dados só poderá ser realizado licitamente, caso esteja subsumido às hipóteses descritas na lei. Os casos de tratamento de dados estão

17 A LGPD circunscreveu a sua incidência a qualquer operação de tratamento de dados pessoais, independente do meio (físico ou digital), realizada no território nacional; bem como quando houver oferta, fornecimento de bens a indivíduos no Brasil ou quando os dados pessoais forem coletados no Brasil, independente do país sede da empresa, ou da nacionalidade das titulares. As exceções à aplicação da lei são restritas e declinadas no artigo 4º da LGPD, que excluiu: i. tratamento realizado por pessoas naturais para fins particulares e não econômicos; ii. atividades jornalísticas, artísticas ou acadêmicas; iii. realizados para fins de: segurança nacional; defesa nacional; segurança do estado ou atividades de investigação e repressão penais; iv) dados provenientes de fora do território nacional e que: não sejam tratados no Brasil; o país de origem proporcione grau adequado de proteção de dados.

18 A LGPD definiu: "Tratamento: toda operação realizada com dados pessoais como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle, modificação, comunicação, transferência, difusão ou extração. " (Art. 5º, XII, Lei 13.709/2018).

elencados na LGPD no art. 7º (dados pessoais)[19]; art. 11 (dados pessoais sensíveis)[20]; artigo 23 (tratamento de dados pelo Poder Público)[21]. Não há nenhuma hierarquia entre as diversas bases normativas, cabendo, apenas, a identificação da mais adequada para dar lastro ao processo de tratamento em cada situação concreta, tendo em vista as características específicas dos dados e as finalidades perseguidas no tratamento.

A LGPD não se fundamenta em uma lógica de restrição ou obstrução à circulação das informações, tanto que contempla um rol extenso e diversificado de bases legais, no qual a competência para iniciar certo processamento de dados pessoais foi atribuída aos agentes de tratamentos[22], que podem exercê-las, prescindindo do consentimento do titular, ao qual, contudo, reserva-se o direito de oposição[23], no caso de descumprimento dos critérios normativos estatuídos na lei.

---

19 O art. 7º da LGPD elenca como hipóteses de tratamento de dados pessoais: i) o consentimento informado do titular; ii) o cumprimento de obrigação legal ou regulatória; iii) pela administração pública, para execução de políticas públicas previstas em lei e regulamento ou respaldada em contratos, convênios ou instrumentos congêneres; iv) realização de estudos por órgão de pesquisa; v) a execução de contrato ou de procedimentos contratuais preliminares; vi) o exercício regular de direito em processo judicial, administrativo ou arbitral; vii) a proteção da vida ou da incolumidade física do titular ou de terceiros; viii) a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ix) para atendimento de interesses legítimos do controlador ou de terceiros; x) para a proteção do crédito.

20 O art. 11 da LGPD indica como bases de tratamento de dados pessoais sensíveis: i) o consentimento específico e destacado do titular; ii) o cumprimento de obrigação legal ou regulatória; iii) pela administração pública, para execução de políticas públicas previstas em lei e regulamento; iv) realização de estudos por órgão de pesquisa; v) o exercício regular de direito em processo judicial, administrativo ou arbitral; vii) a proteção da vida ou da incolumidade física do titular ou de terceiros; viii) a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ix) garantia da prevenção da fraude e segurança do titular.

21 O art. 23 da LGPD prevê o tratamento de dados pessoais pela pessoa jurídica de direito público para o atendimento de sua finalidade pública, com o objetivo de executar as competências legais ou cumprir as suas atribuições constitucionais e legais do serviço público.

22 Conforme a nomenclatura da LGPD, são agentes de tratamento de dados: i. Controlador e o ii. Operador. O *controlador* é quem toma as decisões referentes ao tratamento de dados pessoais, exercendo as competências que legislação lhe confere; ao passo que o *operador* atua como espécie de mandatário do controlador pois realiza o tratamento de dados pessoais em nome dele, de acordo com instruções que lhe forem dadas.

23 O § 2º do art. 18 da LGPD dispõe que: "o titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta lei.".

2.2 Princípios da proteção de dados

O arranjo regulatório da LGPD está estruturado em mandamentos nucleares que organizam axiologicamente a atividade de tratamento de dados, com base na boa-fé objetiva e, por conseguinte, nos deveres de lealdade e cooperação, bem como nos seguintes princípios: i) finalidade; ii) adequação; iii) necessidade; iv) livre acesso; v) qualidade dos dados; vi) transparência; vii) segurança; viii) prevenção; ix) não discriminação e x) responsabilidade e prestação de contas.

Essas normas fundamentais do sistema de proteção de dados prescrevem práticas informacionais equitativas que devem conformar a aplicação do plexo de direitos, deveres e ônus incidentes sobre o fluxo de dados pessoais.

O *princípio da finalidade* tem importância capital no tratamento de dados ao condicionar a licitude dessa atividade à indicação explícita dos propósitos legítimos e específicos do tratamento, que deverão ser previamente informados com clareza ao titular, vedando tratamento posterior incompatível com o individualizado no momento da coleta.

A definição de um propósito legítimo e específico para o tratamento de dados é fundamental para a identificação dos dados que serão necessários à atividade que será desenvolvida, bem como para avaliar a compatibilidade de eventuais usos secundários dos dados com a finalidade originariamente indicada.

A LGPD admite os usos secundários de dados apenas quando houver compatibilidade do tratamento posterior com o propósito legítimo declinado inicialmente pelo controlador. Os possíveis usos congruentes com finalidade originária dependerão de uma análise contextual que pondere de forma justa, tanto a relação fático-jurídica existente entre os atores do processo de tratamento, como também as legítimas expectativas do titular.

Embora a noção de compatibilidade de usos comporte em abstrato certo grau de indeterminação, a base fática da operação e a finalidade inicial são critérios de contenção da discricionariedade do controlador, o qual tem o ônus argumentativo de justificar e prestar contas de maneira transparente do tratamento posterior realizado.

O *princípio da adequação* busca controlar a pertinência do tratamento com as finalidades informadas ao titular em determinado contexto. Para que o controle de adequação seja factível é imprescindível que a finalidade esteja articulada com precisão, e não de maneira genérica, pois pretende-se aferir a correlação entre os dados coletados e o objetivo perseguido. Se não houver congruência lógica nessa relação de meios e fins, não haverá legitimidade na operação de tratamento.

O *princípio da necessidade* limita o tratamento ao mínimo necessário para a realização dos propósitos legítimos declinados. O objetivo desse princípio é restringir a ação intrusiva do controlador ao menor grau possível na coleta de dados, reduzindo-a ao indispensável para o cumprimento da finalidade.

Delimitar qual a quantidade e qualidade de dados que são requeridas para o atendimento de determinado propósito demanda um juízo comparativo dentre os meios disponíveis, para se eleger qual atinge o fim almejado de modo menos oneroso para os direitos fundamentais do titular. Essa redução do tratamento ao mínimo necessário também contribui para mitigar os riscos de danos na hipótese de incidentes de segurança.

O *princípio do livre acesso* assegura aos titulares a consulta facilitada e gratuita sobre a forma e duração de tratamento, bem como à integralidade de seus dados pessoais.

O *princípio da qualidade dos dados* tem por escopo preservar a exatidão, clareza, relevância e a atualização dos dados, assegurando que a identidade do titular reflita-se fielmente na correção dos dados coletados e armazenados, facultando-se a retificação de incorreções eventualmente existentes.

O *princípio da transparência* tem por escopo garantir informações claras, precisas e facilmente acessíveis aos titulares sobre a realização do tratamento e os respectivos agentes de tratamento, preservados os segredos comercial e industrial.

Para que a autodeterminação informacional possa ser exercitada na sua plenitude pelo titular dos dados, a disponibilização ativa de informações é imperiosa, sobretudo nas hipóteses em que o tratamento se realiza sem o consentimento, para

que o titular possa manifestar sua oposição, caso não concorde ou não se observe o regime jurídico adequado.

O *princípio da segurança* prescreve a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados ou situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

O *princípio da prevenção* tem como objeto o risco presente no tratamento de dados e busca a implementação de salvaguardas ou precauções que previnam a ocorrência de danos ou mitigue os seus efeitos no caso de incidentes de segurança.

O *princípio da não discriminação* prescreve a interdição do tratamento de dados com fins discriminatórios ilícitos ou abusivos, visto que, em muitas situações, classificações e segmentações, com base no tratamento de dados, são justificáveis e necessárias para execução de políticas públicas destinadas a corrigir desigualdades sociais com foco nos grupos sociais desfavorecidos.

Para prevenir o risco de discriminações ilícitas ou abusivas, tutelam-se, com medidas precaucionarias mais restritas, os dados pessoais qualificados como sensíveis por serem mais suscetíveis de utilização abusiva com prejuízo à isonomia.

O *princípio da responsabilização e prestação de contas* preceitua o dever de demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas na prevenção e mitigação de riscos ou reparação de danos.

Como os agentes de tratamento tomam decisões no procedimento de circulação das informações, interpretando e aplicando conceitos jurídicos indeterminados, são-lhes impostos deveres de prestar contas, explicitando as escolhas realizadas, que afetam os direitos fundamentais dos titulares (*accountability*)[24].

24 Para um exame do princípio da *accountability* na regulação e proteção de dados, ver Bioni (2022).

2.3 Dados pessoais

A LGPD definiu *dado pessoal* como a informação[25] relacionada à pessoa identificada ou identificável (art. 5º, inc. II), adotando um conceito amplo ao utilizar o vocábulo "identificável". Trata-se de um conceito central, pois é o elemento de conexão que atrai a aplicação do regime jurídico de proteção de dados para uma situação concreta.

Por *pessoa "identificada*" entende-se a situação em que há a vinculação de determinado elemento de identificação com o indivíduo de forma direta, como o próprio nome ou atributos biográficos numéricos únicos (número de inscrição no Cadastro de Pessoa Física – CPF) etc.

Já *pessoa "identificável*" comporta um incalculável número de elementos que, uma vez processados e associados, permitem a identificação de determinado indivíduo.

O dado referível à pessoa humana viva com aptidão para individualizá-la, direta ou indiretamente, qualifica-se como dado pessoal. O legislador, ao mencionar pessoa natural "identificável" ao lado das identificadas, adotou um conceito de grande latitude para expandir ao maior grau a aplicabilidade da tutela jurídica aos dados relacionados às pessoas, assegurando aos indivíduos a participação no processo de circulação de informações que lhes dizem respeito[26].

2.4 Danos anonimizados

Em contraste com os dados pessoais, a LGPD também alude aos *dados anônimos*, isto é, os dados pessoais que passaram por processo técnico que os

25 A legislação menciona dado e informação de maneira sobreposta, embora a rigor haja uma distinção entre eles que se costuma fazer no campo das normas técnicas computacionais. O dado seria uma informação em potencial que pode converter-se em informação (Waks, 1989, p. 25 *apud* Doneda, 2006), estando "associado a uma espécie de 'pré-informação' anterior à interpretação e ao processo de elaboração" (Doneda, p. 2006, 152). Dados seriam signos representativos de certos fatos que, uma vez processados ou interpretados, transformam-se em informações. Contudo, o legislador e a literatura mencionam amiúde os dois termos com significações próximas ou sinônimas.

26 Como preleciona Bioni (2021, p.65) "proteção dos dados pessoais, como um novo direito da personalidade, dirige-se a todo e qualquer dado em que se denote o *prolongamento* de um sujeito. Dados pessoais não se limitam, portanto, a um tipo de projeção *imediata*, mas, também, a um referencial *mediato* que pode ter *ingerência* na esfera de uma pessoa.

desvincularam de determinada pessoa ao qual estavam originariamente relacionados. Trata-se da anonimização que se define como a "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. 5º, inc, XI, Lei 13.709/2018).

A LGPD preceituou que os dados anonimizados estão excluídos do seu campo de incidência, salvo se o processo de anonimização puder ser revertido com esforços razoáveis ou com meios próprios do controlador. A resiliência do processo de anonimização depende da aferição, em determinado contexto, do que seja "esforço razoável", o qual deve ser avaliado em consonância com o estado da arte da tecnologia requerida para a engenharia reversa, considerando o custo e tempo empregados para a execução da atividade (Bioni, 2021, p. 61-72).

2.5 Dados pseudoanonimizados

Entre os dados pessoais e os anônimos, a LGPD faz alusão também à categoria dos *dados pseudoanonimizados*, que corresponde ao dado tratado que perdeu a possibilidade de associação a um indivíduo, senão pelo uso de informação suplementar, custodiada apartadamente pelo controlador em ambiente seguro e restrito.

Trata-se de uma técnica de anonimização de reversão factível, a qualquer momento, com o uso de informações adicionais, que são guardadas separadamente pelo agente de tratamento, razão pela qual os dados pseudoanonimizados mantêm a condição de dado pessoal, pois a reidentificação do indivíduo é facilmente realizada pelo controlador. Esse mascaramento ou ocultação de identificadores tem o condão de mitigar riscos na atividade de tratamento de dados, sobretudo na hipótese de incidentes de segurança[27].

27 A LGPD prescreve que, sempre que for possível, os dados utilizados em pesquisa deverão ser objeto de anonimização ou pseudoanonimização (arts. 7º, IV; 11, II, "c", 12 e 16).

2.6 Dados sensíveis

Na sociedade informacional, um dos grandes desafios enfrentados pela tutela jurídica dos dados pessoais é o fenômeno da "datificação" (representação em *bits* da vida de uma pessoa), que pode dar azo a uma "biografia digital" (Solove, 2004, p. 44) distorcida pelo uso inapropriado de dados pessoais (perfil digital incongruente com a identidade real da própria pessoa), afetando o livre exercício de liberdades fundamentais ou o usufruto de oportunidades sociais em detrimento da igualdade, por conta de classificações estereotipadas ou práticas discriminatórias.

Ciente desse risco, o legislador destinou peculiar atenção para uma categoria especial de dados, qualificada como *dados sensíveis*, cujas informações revelam a 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, quando vinculado a uma pessoa natural.

Esses dados são tratados com maior rigor e protegidos por salvaguardas adicionais, especialmente com monitoramento mais restrito da sua circulação[28] ou a proibição de compartilhamento em certas circunstâncias[29], pois podem dar margem a discriminações e estigmatizações, em detrimento do direito à isonomia. Requer consentimento específico e destacado do titular, bem como as bases legais para tratamento são mais restritivas do que os dados pessoais triviais.

O critério para a seleção dos dados sensíveis não seria apenas a possibilidade de revelar fatos relacionados à intimidade da pessoa, mas principalmente o risco de discriminações abusivas que cerceiem o campo de escolhas dos indiví-

28 De acordo com o art. 11, § 3º da LGPD, Autoridade Nacional de Proteção de Dados poderá vedar ou regulamentar a comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica.

29 A LGPD proibiu a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto em hipóteses restritas em benefício do titular (art. 11, § 4º); bem como também expressamente vedou às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários" (art. 11, § 5º).

duos. Como sublinha Doneda (2006, p. 162) "um dado, em si, não é perigoso ou discriminatório – mas o uso que dele se faz pode sê-lo". Por isso, é preciso estar atento à natureza mutante dos dados pessoais decorrente de aplicação de tecnologias de extração e análise, que pode convertê-los de dados pessoais triviais para sensíveis, conforme o estado da arte da tecnologia de processamento de informações em determinada época.

2.7 Dados públicos e dados manifestamente públicos

A LGPD regulou os *dados pessoais, cujo acesso é público*[30]; bem como os *dados tornados manifestamente públicos pelo titular*[31]. Nas duas hipóteses os dados pessoais encontram-se disponíveis ao público. O que as distingue é a forma como foram divulgados. Na primeira, os dados pessoais foram expostos ao público por terceiros com base em normas jurídicas que impuseram tal publicidade[32]. Na segunda, a decisão de tornar público é do próprio titular (publicações em redes sociais de perfil aberto).

O fato de os dados pessoais encontrarem-se abertos ao público não significa que se converteram em *res nullius*, isto é, coisa de ninguém que pode ser apropriada e utilizada à revelia dos direitos do seu titular. Ao contrário, tais dados continuam vinculados à pessoa natural de quem são emanações e o processamento posterior deles para novas finalidades só será possível, desde que sejam observados propósitos legítimos e específicos para o novo tratamento, preservados os direitos do titular, os fundamentos e os princípios da LGPD.

Se não houver base legal para o tratamento posterior com amparo na LGPD, constitui ilicitude o processamento deles com base no singelo argumento de que são de acesso público, pois é importante avaliar a finalidade, a boa-fé e eventual

30 Art. 7º, § 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

31 Art. 7º, § 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.

32 O princípio constitucional da publicidade determina a divulgação de informações de interesse público pelo Estado, o que pode levar a circulação pública de dados pessoais de indivíduos que se relacionam com órgãos da administração em situações que tal transparência é necessária para o controle social.

interesse público que justificaram a divulgação dos dados pessoais, bem como as legítimas expectativas do titular, considerando o contexto no qual se deu a divulgação dos dados.

A LGPD não disciplina os dados pessoais com base na dicotomia entre o público o privado, que reservava proteção apenas para dados pessoais privados confidenciais, que se encontravam no campo da privacidade. Essa não é a racionalidade da lei, que considera passível de amparo qualquer tipo de dado pessoal, pois todos são relevantes (Bioni, 2021, p. 267).

Essa tutela se vê confirmada no caso dos dados pessoais que se acham disponíveis ao público, pois a reutilização deles, segundo Bioni (2021, p. 267), "deve levar em consideração o contexto pelo qual tais dados são publicamente acessíveis". Eventual compatibilidade de tratamento posterior exigirá uma análise contextual para saber por que houve publicização da informação, o que calibrará os possíveis (re)usos que dela podem ser feitos" (Bioni, 2021, p. 68).

2.8 Tratamento de dados e atividade jurisdicional

A LGPD alcança as atividades desenvolvidas pelos órgãos do Poder Judiciário (Tribunais), que realizam o tratamento de dados pessoais, exercendo a função de controlador, em nome da pessoa jurídica de direito público ao qual estiverem vinculados[33], pois são responsáveis pelas principais decisões relativas ao tratamento de dados pessoais na execução das suas atividades ou realizadas por terceiros (operadores), segundo suas instruções.

O tratamento de dados pessoais pelo Judiciário ocorre tanto na atividade-meio[34] como na atividade-fim, realizando-o, na maior parte dos casos, indepen-

33 Os tribunais federais atuam em nome da União, ao passo que os tribunais estaduais em nome do Estado que exercer a atividade jurisdicional.

34 Também para gestão da atividade-meio, que dá suporte às atividades jurisdicionais, haverá a obrigação de processar dados pessoais de magistrados, servidores e colaboradores, incluindo empregados de empresas terceirizadas e estagiários, pensionistas e dependentes de servidores, visitantes das dependências do Tribunal. Em suma, há uma variada gama de relações jurídicas imprescindíveis para o funcionamento do sistema de justiça para qual o tratamento de dados será exigido, seja para o cumprimento de obrigações legais e regulatórias, seja para execução de contratos com prestadores de serviços.

dentemente do consentimento do titular. A prestação dos serviços jurisdicionais de resolução de conflitos, prevista na Constituição e legislação processual, implica necessariamente o tratamento de dados pessoais das partes, advogados, magistrados, membros do Ministério Público e da Defensoria Pública, auxiliares e colaboradores da Justiça, além de eventuais operadores do direito que atuem em processos judiciais físicos ou eletrônicos.

Para o exercício de sua competência jurisdicional e administrativa, os órgãos do Judiciário poderão coletar, armazenar e usar determinadas categorias de informações pessoais, tais como: dados de identificação pessoal e contato; informações de login; dados financeiros; registros de vídeo, imagem e voz. Também, poderão ser tratados dados pessoais sensíveis, como os dados biométricos; dados referentes à saúde; dados que revelam filiação a sindicato; dados relacionados à origem racial ou étnica; entre outros que podem ser expostos em processos judiciais ou administrativos.

A base legal para processamento de dados na atividade-fim do Judiciário encontra-se no artigo 23 da LGDP, que prevê a possibilidade de tratamento de dados pelas pessoas jurídicas de direito público para desincumbir-se das missões constitucionais e cumprir atribuições legais de serviço público que lhe foram impostas pelo ordenamento jurídico.

Esse tratamento de dados por pessoas jurídicas de direito público está condicionado, de acordo com o inciso I do art. 23 da LGPD, a um dever de transparência ativa com a divulgação de informações claras e atualizadas, preferencialmente em seus sítios eletrônicos, relativas às hipóteses e às finalidades nas quais se realizam o tratamento de dados pessoais no exercício de suas competências institucionais.

O princípio da publicidade dos atos processuais impõe também o dever de tornar públicos alguns dados pessoais no âmbito do processo judicial eletrônico. Na próxima seção será analisada a necessidade de balancear as normas relativas a publicidade processual e a proteção de dados pessoais.

3. PROCESSO JUDICIAL ELETRÔNICO E PROTEÇÃO DE DADOS

3.1 Princípio da publicidade na Administração Pública

O princípio da publicidade encontra-se previsto na Constituição no artigo 37 como norma estruturante da Administração Pública e como um dos pilares do estado democrático de direito e da concepção republicana de poder. Em uma República, todo poder jurídico-político deriva da soberania popular. Esse poder pode ser exercido diretamente pelos cidadãos, por meio dos mecanismos da democracia direta, ou, indiretamente, por meio dos representantes que são eleitos para gestão da coisa pública, quer no legislativo, quer no Executivo.

O exercício do poder de modo transparente, instrumentalizado pela publicidade, é fundamental ao regime democrático pois, segundo Bobbio, a "*res pública* não apenas no sentido próprio da palavra, mas também no sentido de exposto ao público exige que o poder seja visível" (Bobbio, 1999, p. 31), permitindo o controle social da atividade estatal.

Complementado o princípio constitucional da publicidade, há normas constitucionais que garantem aos cidadãos o acesso a "registro administrativos e a informações sobre os atos de governo" (art. 37, II), bem como o direito de receber do Estado informações de seu interesse particular, ou de interesse coletivo ou geral. A regra, portanto, é a visibilidade da atividade pública, admitindo-se o sigilo apenas quando seja imprescindível à segurança da sociedade e do Estado (art. 5º, XXXIII, CF) ou proteção da privacidade dos cidadãos (art. 5º, X e XII, CF).

Esse dever do Estado de atuar para garantir o direito fundamental de acesso à informação encontra-se regulamentado na Lei 12.527/2011 que determina: i) publicidade como preceito geral e do sigilo como exceção; ii) divulgação de informações de interesse público, independentemente de solicitações; iii) utilização de meios de comunicação viabilizados pela tecnologia da informação; iv) fomento ao desenvolvimento da cultura de transparência na administração pública; v) desenvolvimento do controle social da administração pública.

Busca essa legislação viabilizar uma cidadania participativa que interaja com a Administração Pública com base em informações de qualidade que devem ser franqueadas ativamente como meio de assegurar a cultura de transparência pública que reduza a assimetria informacional entre os administrados e o poder público[35].

O dever de publicar nos órgãos oficiais de divulgação (Diário Oficial) as leis, atos e decisões administrativas que afetam a esfera de direitos de terceiros também se relaciona com a ideia de publicidade, como obrigação procedimental indispensável para a validade e eficácia de tais atos. Este tipo de publicidade tem o escopo de gerar a presunção absoluta de que seus destinatários conhecem tais atos estatais, não podendo arguir a sua ignorância para escusar-se do seu cumprimento.

3.2 Publicidade processual na atividade jurisdicional

A atividade jurisdicional também se encontra sujeita a deveres especiais de publicidade. Embora a magistratura não seja eleita, ela exerce, em nome do povo, parcela do poder do Estado na resolução de litígios, devendo atuar com independência e imparcialidade na aplicação da lei.

O exercício dessa função pública de forma íntegra e isenta também deve ser realizado com transparência para que a sociedade possa exercer democraticamente a fiscalização e o controle externo e difuso, vedando-se, assim, a opacidade institucional que gera desconfiança sobre legitimidade das atividades da magistratura[36].

---

35 Na doutrina distingue-se o princípio da publicidade do princípio da transparência que muitas vezes são tratados como sinônimos (Arruda, 2020; Martins Junior, 2010). Embora tais princípios (publicidade e transparência) possuam pontos comuns, o princípio da transparência condessaria outros valores, além da visibilidade do poder público, ao postular uma governança com a participação informada dos administrados (consultas e audiências públicas), bem como um dever ativo de prestar contas (*accountability*), com a devida motivação das decisões administrativas. Como explica Galetta (2018, p.141) "la transparencia es ciertamente un concepto multipropósito y de contenido indefinido. Como ya se ha señalado, la transparencia no se agota con el derecho de acceso a la información pública y no se acaba con el cumplimento de este derecho. Hay otros instrumentos esenciales en este sentido, como confirma un análisis de derecho comparado: se trata, em particular, de la participación en los procedimientos y de la obligación de motivación de los actos públicos."

36 Conforme preleciona Greco (2002, p. 41), "a publicidade dos atos processuais é uma das mais importantes garantias do processo democrático, pois é o único instrumento eficaz de controle da exação dos juízes no cumprimento

Além de a publicidade processual ter a função de conferir visibilidade, fomentando o controle social das ações do Poder Judiciário (publicidade externa), ela também cumpre, no interior do processo (publicidade interna), a finalidade de garantir o desenvolvimento justo e equitativo dessa atividade ao dar ciência às partes dos atos e fatos processuais, bem como das decisões proferidas, conforme exige o princípio do contraditório e do devido processo legal[37].

A regra é a publicidade processual ampla da atividade jurisdicional, que não se limita à presença nos julgamentos ou divulgação das decisões, mas abrange o acesso integral ao conteúdo do processo, sendo a exceção o sigilo. No julgamento da ADI 4414/AL, o Supremo Tribunal decidiu que "a publicidade assegurada constitucionalmente (art. 5º, LX, e 93, IX, da CRFB) alcança os autos do processo, e não somente as sessões e audiências, razão pela qual padece de inconstitucionalidade a disposição normativa que determine abstratamente o segredo de justiça em todos os processos em curso perante a Vara Criminal. " .

3.3 Restrições à publicidade processual

Conquanto a publicidade processual seja um valor necessário para o desenvolvimento de um processo justo, ela não é absoluta, tendo sido conferido ao legislador a faculdade de restringi-la, quando a *defesa da intimidade* ou *interesse social* relevante justificar tal medida, que deve ser sopesada com o *interesse público à informação*, além de se permitir que se limite a presença em determinados atos às próprias partes e a seus advogados, ou somente a estes.[38]

---

dos seus deveres e no respeito à dignidade humana e aos direitos das partes. Por isso, dela depende a credibilidade e a confiança que a sociedade deve depositar na Justiça. *Justice is not only to be done, but to be seen to be done*. Toda vez em que ela é suprimida através do segredo de justiça, fica sob suspeita a exação do juiz.".

37 De acordo com art. 93, IX, da CF, "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".

38 A legislação processual penal contempla no artigo 217 do CPP a possibilidade de retirada do réu da sala de audiência, quando o juiz verificar que a presença dele no ato poderá causar humilhação, temor, ou sério constrangimento à testemunha ou ao ofendido, prejudicando a veracidade do depoimento. Em tal situação, a inquirição será realizada, com a presença do seu defensor, caso ela não possa ser realizada por videoconferência.

Essas situações excepcionais de sigilo encontram-se discriminadas especialmente na legislação processual civil e penal. Trata-se de matéria submetida ao princípio da reserva legal e de jurisdição.

O legislador adota dois critérios na legislação processual civil para delimitar as exceções à regra de que atos processuais são públicos. Ora define objetivamente os processos que tramitam sob segredo de justiça (segredo *ope legis*)[39], com base na natureza do litígio tratado neles; ora atribui ao magistrado (segredo *ope judicis*)[40] a competência para, motivadamente, decidir pela imposição de sigilo, a fim de resguardar a intimidade das partes ou interesses gerais da coletividade, comportando em tais situações a ponderação entre bens e valores colidentes (interesse público à informação *versus* proteção da intimidade), com amparo no princípio da proporcionalidade, garantindo, todavia, em qualquer caso a presença das partes e dos seus advogados.

Esse modelo de publicidade processual ampla foi projetado pelo legislador para uma realidade processual em que os registros das informações processuais ocorriam em autos cartáceos – físicos – cujo conhecimento integral do seu conteúdo requeria o deslocamento dos interessados às unidades judiciarias.

Segundo Cueva (2019, p. 138), esse fenômeno restou conhecido como "obscuridade prática dos documentos de papel", visto que o acesso aos dados processuais era custoso e demorado. Porém, tal cenário modificou-se radicalmente com a implantação do processo judicial eletrônico que centraliza em um único banco de dados todas as informações processuais dos litigantes e litígios em determinado tribunal.

O § 1º do artigo 792 do CPP também prevê hipótese de restrição de acesso, se da publicidade da audiência, da sessão ou do ato processual, puder resultar escândalo, inconveniente grave ou perigo de perturbação da ordem, o juiz, ou o tribunal, câmara, ou turma, poderá, de ofício ou a requerimento da parte ou do Ministério Público, determinar que o ato seja realizado a portas fechadas, limitando o número de pessoas que possam estar presentes.

39 O artigo 189, II e IV do CPC prevê que tramitam em segredo de justiça os processos que i) versem sobre casamento, separação de corpos, divórcio, separação, união estável, filiação, alimentos e guarda de crianças e adolescentes; ii) versem sobre arbitragem, inclusive sobre cumprimento de carta arbitral, desde que a confidencialidade estipulada na arbitragem seja comprovada perante o juízo.

40 Também prevê o art. 189 do CPC, incisos I e III a possibilidade de o segredo de justiça ser casuisticamente decretado nos casos i) em que o exija o interesse público ou social; ii) em que constem dados protegidos pelo direito constitucional à intimidade. Porém, a decisão que determina o segredo de justiça deve ser adequadamente motivada, com fundamento em circunstâncias especiais claramente identificadas e estritamente necessárias.

3.4 Processo judicial eletrônico: dados abertos e autodeterminação informacional

A mudança do modo de compilação de informações processuais do processo físico em papel para os autos eletrônicos tem como marco legal autorizador a Lei 11.419/2006. Em 2013, o Conselho Nacional de Justiça, pela Resolução 185/2013, regulamentou e fixou parâmetros para o Sistema Processo Judicial Eletrônico – PJE, como mecanismo central de informatização e digitalização dos processos judiciais para ampliar a celeridade e eficiência dos serviços jurisdicionais. Este intenso processo de transformação digital[41] da justiça recolocou o problema da privacidade e da autodeterminação informacional, garantidos pela LGPD, em face de uma política de dados abertos à sociedade, que pode acarretar uma exposição desnecessária de dados pessoais e sensíveis das pessoas naturais que litigam no Judiciário.

A política de acesso ao processo judicial eletrônico pela rede mundial de computadores está ordenada na Lei 11.419/2006, no Código de Processo Civil e também em atos normativos expedidos pelo Conselho Nacional de Justiça, especialmente nas Resoluções 121/2010 e 185/2013.

Ressalvados os processos que tramitam em segredo de justiça, cujo acesso é garantido apenas às partes e aos procuradores constituídos nos autos, nos demais processos prevalece a regra geral da publicidade processual.

Contudo, o acesso ao conteúdo integral do processo judicial eletrônico, inclusive de documentos anexados, pela rede mundial de computares não é aberto a todas as pessoas, mas só aos advogados em geral, membros do Ministério Público e magistrados, ainda que não sejam vinculados ao processo a ser examinado, desde que estejam cadastrados no sistema e demonstrem interesse

41 O Relatório Justiça em Números de 2023 do CNJ informa que "85,8% dos processos em tramitação eram eletrônicos ao final do ano de 2022, com indicadores de 89,3% no segundo grau, de 85,4% no primeiro grau e de 100% nos Tribunais Superiores. A Justiça Eleitoral e a Justiça do Trabalho se destacam por apresentarem diversos tribunais com 100% de processos eletrônicos, tanto no primeiro, como no segundo grau". Disponível: https://www.cnj.jus.br/wp-content/uploads/2023/08/justica-em-numeros-2023.pdf. Acesso em 15/03/2024

para fins apenas de registro, conforme estatuído nos § § 6º e 7º do art. 11 Lei 11.419/2006[42], bem como pelo art. 3º da Resolução 121/2010[43]. Logo, a consulta aos autos do processo eletrônico poderá ser feita pelo público em geral nos casos que não tramitam em segredo de justiça, sem a necessidade de cadastro, apenas nas secretarias dos órgãos judiciários, conforme prescrito pelo § 1º do art. 27 da Resolução 185/2013[44] do CNJ.

O que se disponibiliza amplamente pela rede mundial de computadores a toda e qualquer pessoa, independentemente do prévio cadastramento ou de demonstração de interesse, é a consulta aos dados básicos dos processos judiciais, de acordo com o art. 2º da Resolução 121/2010 do CNJ, que são os seguintes: i) número, classe e assuntos do processo; ii) nome das partes e de

---

42 A Lei 13.793/2019 modificou as Leis n os 8906/1994, 11.419/2006, e 13.105/2015 (Código de Processo Civil), para deixar explícito o direito de os advogados examinarem, mesmo sem procuração, atos e documentos de processos e de procedimentos eletrônicos, independentemente da fase de tramitação, bem como a obterem de cópias, salvo nas hipóteses de sigilo ou segredo de justiça, nas quais apenas o advogado constituído terá acesso aos atos e aos documentos referidos.

O art. 11 da Lei nº 11.419/2006 passou a vigorar com as seguintes alterações nos §§ 6º e 7º:

§ 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.

§ 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.

43 Art. 3.º O advogado cadastrado e habilitado nos autos, as partes cadastradas e o membro do Ministério Público cadastrado terão acesso a todo o conteúdo do processo eletrônico.

§ 1º. Os sistemas 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 sigilo ou segredo de justiça.

§ 2º. Deverá haver mecanismo que registre cada acesso previsto no parágrafo anterior.

44 Art. 27. A consulta ao inteiro teor dos documentos juntados ao PJe somente estará disponível pela rede mundial de computadores, nos termos da Lei n. 11.419, de 19 de dezembro de 2006, e da Resolução CNJ n. 121, de 5 de outubro de 2010, para as respectivas partes processuais, advogados em geral, Ministério Público e para os magistrados, sem prejuízo da possibilidade de visualização nas Secretarias dos Órgãos Julgadores, à exceção daqueles que tramitarem em sigilo ou segredo de justiça.

§ 1º Para a consulta de que trata o caput deste artigo será exigido o credenciamento no sistema, dispensado na hipótese de consulta realizada nas secretarias dos órgãos julgadores.

seus advogados; iii) movimentação processual; iv) inteiro teor das decisões, sentenças, votos e acórdãos.

Tanto os dados básicos franqueados a toda e qualquer pessoa na rede mundial de computadores, quanto o acesso aos autos eletrônicos, que não se encontram sob o segredo de justiça, a todos os advogados cadastrados no sistema informatizado da justiça, tornam público e acessível a terceiros volumes incomensuráveis de dados pessoais e sensíveis das pessoas naturais que participam dos processos judiciais eletrônicos, os quais podem ser coletados por *crawlers* (robôs rastreadores), que cumprem a função de realizar a varredura em sítios eletrônicos ou em bancos de dados digitais, para realizar mineração e extração de informações (*web scraping*).

Tais dados podem ser tratados com tecnologias computacionais algorítmicas com intensa capacidade de volume, velocidade e variedade (*Big Data* e *data agregation*), que são capazes de estabelecer correlações e fazer predições por conta do alto poder de agregação, inferindo-se tendências e preferências dos seus titulares, o que permite a projeção de perfis comportamentais por *data brokers*, organizações especializadas em processar dados pessoais de múltiplas fontes, para comercialização com diversos objetivos (publicidade personalizada, prevenção à fraude, etc).

Em suma, tais dados podem ser reutilizados para propósitos diferentes dos que justificaram a sua coleta, sem o consentimento dos seus titulares, que perdem o controle sobre eles, em detrimento da autodeterminação informacional.

Esses dados também permitem que os cidadãos que buscam a Justiça sejam classificados e possam ser vítimas de discriminações, com base nas informações que foram coletadas nesses processos. É por isso que, no âmbito da Justiça do Trabalho, procura-se obstaculizar o acesso aos dados que identifiquem as partes do processo[45], a fim de evitar "catalogações" e a formação de "lista de indesejáveis", passíveis de serem consultadas em processos seletivos, prejudicando, dessa

45 O artigo 4º da Resolução 121/2010 do CNJ excepciona os processos sujeitos à apreciação da Justiça do Trabalho da consulta pública nos sistemas de tramitação e acompanhamento processual, por meio da rede mundial de computadores, com base no nome das partes ou número de registro no cadastro de contribuintes do Ministério da Fazenda – CPF.

forma, o acesso ao mercado de trabalho de pessoas que exercitaram o direito de acionar eventual empregador.

Como já decidido pelo STF na ADI 6387/DF, quando reconheceu o princípio da autodeterminação informacional e o *status* de direito fundamental à proteção de dados, não há dados pessoais irrelevantes, pois todos têm importância e valor, bastando que seja uma informação relacionada à pessoa natural identificada ou identificável. Mesmo que, em um primeiro momento, tais dados não sejam referíveis diretamente a alguém, uma vez compartilhados, cruzados ou organizados, podem converter-se em dados bastante específicos, revelando, inclusive, informações sensíveis sobre ela. É para minorar o risco de danos às pessoas que se recomenda, sempre que possível, a utilização de técnicas de anonimização ou pseudoanonimização dos dados, desvinculando-os da pessoa da qual emanam.

Como relata Cueva (2019), em países europeus tem-se buscado conciliar a publicidade processual e a abertura de dados judiciais com a legislação de proteção de dados, utilizando-se da técnica de pseudoanonimização para obscurecer dados de identificação das partes e de seus advogados, assim como detalhes dos autos que permitam extrair informações de cunho pessoal.

A LGPD refere-se à pseudoanonimização como ferramenta para mitigação de riscos que faculta ao controlador desvincular um dado pessoal de determinado indivíduo. A Resolução 334/2020 do CNJ, que instituiu o Comitê de Dados Abertos e Proteção de Dados no âmbito do Poder Judiciário, menciona a necessidade de proteger a personalidade e autodeterminação informativa da pessoa contra os riscos decorrentes do acesso massificado a informações contidas em processos judiciais, indicando, entre as propostas destinadas a preservar direitos e garantias previstos na LGPD: i) “medidas técnicas e administrativas para proteção dos elementos identificadores de pessoas naturais, tais como pseudoanonimização, anonimização, acesso restrito ou ocultação”; ii) medidas de gerenciamento e limitação do acesso massificado aos documentos juntados pe-

las partes, considerando os riscos aos titulares de dados pessoais". Porém, até o momento, não foram implementadas essas funcionalidades no processo judicial eletrônico para proteger dados pessoais de identificação das pessoas naturais que figurem como partes processuais.

Importante ponderar que a adoção dessa providência (restrição de acesso aos dados de identificação das partes dos processos judiciais pela via da pseudoanonimização) não compromete a finalidade da publicidade processual externa, que objetiva viabilizar o controle social da atividade jurisdicional. É possível compreender, avaliar e criticar os pronunciamentos jurisdicionais, ainda que não sejam conhecidas as partes da relação processual.

Contudo, havendo interesses legítimos que justifiquem a prevalência da ampla publicidade, incluindo os dados de identificação dos sujeitos do processo, seria possível a reversão da pseudoanonimização, pois o controlador (Judiciário) disporia de condições técnicas para a reidentificação.

É possível conciliar uma política de dados abertos que maximize o controle democrático da atividade do Estado, inclusive do Judiciário, mas que também proteja dados pessoais dos cidadãos, preservando a exposição deles, quando não sejam indispensáveis à consecução de propósitos públicos prescritos pelo ordenamento jurídico, conforme estabelecido pelos princípios da finalidade, necessidade e adequação previstos na LGPD, como parâmetros para a aferição da proporcionalidade no tratamento de dados pessoais.

Poder-se-ia argumentar que a publicidade externa, com identificação das partes processuais, protegeria potenciais interesses de terceiros de conhecer a existência de tais litígios para avaliar os riscos jurídicos e econômicos que incorreriam, caso entabulassem relações e negócios com os litigantes. Esse argumento, porém, não é plausível, pois o legítimo interesse de terceiros de mapear tais riscos podem ser averiguado com mais precisão pelo canal de expedição de certidões, nas quais as partes e objeto da lide são identificados, como atualmente já se realiza com mais segurança jurídica, e não pela difusão de informações pessoais na rede mundial de computadores.

Com relação aos dados sensíveis, contidos em documentos, petições ou atos processuais registrados nos processos judiciais eletrônicos, há mecanismo próprio para resguardá-los, quando for necessário, como a decretação de sigilo parcial do ato ou documento. Essa providência pode ser requerida pela parte no momento da apresentação dos dados no processo judicial eletrônico, cabendo ao magistrado avaliar ulteriormente se mantém a pretensão de confidencialidade[46].

O dado sensível *per se* não conduz o processo inexoravelmente ao sigilo, pois, em cada caso, caberá ao juiz apreciar a necessidade e a pertinência da sua decretação, considerando o interesse público, social ou direito constitucional à intimidade, que justificariam o ocultamento dessa informação[47]. Impende recordar que a LGPD não trata de sigilo de dados, mas sim do uso controlado deles na sociedade pelo seu titular.

CONSIDERAÇÕES FINAIS

A LGPD regulamentou de maneira transversal a problemática da proteção de dados, com objetivo de garantir a autodeterminação informacional dos cidadãos, que devem ter controle sobre o fluxo dos dados que lhes são pertinentes, os quais são projeções da sua personalidade.

---

46 Em seu art. 28 Resolução 185/2013 do CNJ prevê a competência para a parte interessada impor sigilo total ou parcial do processo, o que será apreciado ulteriormente pelo juiz.
Art. 28. Na propositura da ação, o autor poderá requerer segredo de justiça para os autos processuais ou sigilo para um ou mais documentos ou arquivos do processo, através de indicação em campo próprio.
§ 1º Em toda e qualquer petição poderá ser requerido sigilo PARA esta ou para documento ou arquivo a ela vinculado.
§ 2º Requerido o segredo de justiça ou sigilo de documento ou arquivo, este permanecerá sigiloso até que o magistrado da causa decida em sentido contrário, de ofício ou a requerimento da parte contrária.
§ 3º O Tribunal poderá configurar o sistema de modo que processos de determinadas classes, assuntos ou por outros critérios sejam considerados em segredo de justiça automaticamente.

47 Nessa linha, o Enunciado 681, aprovado na IX Jornada de Direito Civil, promovido pelo Conselho da Justiça Federal (CJF): "A existência de documentos em que há dados pessoais sensíveis não obriga à decretação do sigilo processual dos autos. Cabe ao juiz, se entender cabível e a depender dos dados e do meio como produzido o documento, decretar o sigilo restrito ao documento específico." Disponível:https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciario1/publicacoes-1/jornadas-cej/enunciados-aprovados-2022-vf.pdf. Acesso em: 04 de fev. 2021.

Esse marco legal não se não se fundamenta em uma dicotomiaentre o público e o privado, que está na origem da tutela legal e constitucional da privacidade, que tinha por escopo apenas dados relacionados à vida privada e íntima. Para a LGPD é suficiente que o dado seja ajustado para "relacionado a uma pessoa humana viva, identificada ou identificável para ser valioso e tutelado em todo o seu ciclo vital, a fim de prevenir o seu uso ilícito ou abusivo por terceiros.

A LGPD não se limita à proteção do sigilo de dados, tampouco trabalha com uma lógica obstrutiva à sua circulação. Ao contrário, busca-se organizar o apropriado fluxo informacional de modo justo e equitativo, procura mitigar vulnerabilidades e reduzir as assimetrias de poder inerentes ao tratamento de dados na sociedade digital.

O processo judicial eletrônico, com a centralização de todas as informações processuais em banco de dados digitais, produziu mudanças sócio técnicas que recolocaram o problema da publicidade processual ampla e a necessidade de sua harmonização com autodeterminação informacional dos participantes do processo judicial, conforme previsto na LGPD.

Discutiu-se a necessidade da difusão de dados pessoais das partes processuais na rede mundial de computadores, tendo-se argumentado que seria mais consentâneo com os princípios da LGPD a adoção de mecanismos mitigadores dessa excessiva exposição, como a pseudoanonimização de dados pessoais de identificação dos litigantes, a fim de evitar o potencial uso abusivo desses elementos para a formação de perfis informacionais dos jurisdicionados.

Com relação aos dados sensíveis, incluídos em documentos ou atos processuais, o processo judicial eletrônico já dispõe de medida técnica própria, que seria o sigilo processual restrito ao ato ou documento veiculador da informação sensível que se pretende proteger, devendo esse risco ser aferido casuisticamente, ponderando os interesses e valores colidentes.

REFERÊNCIAS

ARRUDA, Carmen Silvia L. **O princípio da transparência**. 1ª ed., São Paulo: Quartier Latin, 2020.

BIONI, Bruno R. **Proteção de dados pessoais: a função e os limites do consentimento**. 3ª ed., Rio de Janeiro: Forense, 2021.

BIONI, Bruno R. **Regulação e a Proteção de dados**: o princípio da accountability. 1ª ed., Rio de Janeiro: Forense, 2022.

BOBBIO, Norberto. **Estado, governo e sociedade**; **para uma teoria geral da política**. Trad. Marco Aurélio Nogueira. 7ª ed., Rio de Janeiro: Paz e Terra, 1987.

CASTELLS, Manuel. **A sociedade em rede**. Trad.: Roneide Venâncio Majer. 25ª ed., Rio de Janeiro: Paz e Terra, 2023.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Justiça em números 2023**. Brasília: CNJ, 2023. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2023/08/justica-em-numeros-2023.pdf. Acesso em 15/03/2024.

CUEVA, Ricardo V. L. Proteção de dados pessoais no judiciário. **Revista do Advogado** 2019 v. 39 n. 144 nov, pp. 134-140.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: **Renovar**, 2006.

GALETTA, Diana-Urania. **Transparencia y buen gobierno**. Evaluación y propuestasa partir de la experiencia en la Unión Europea e Italia. *Dilemata* - Revista Internacional de *Éticas Aplicadas*, n. 27, 2018. Disponível em <https://www.dilemata.net/revista/index.php/dilemata/article/view/412000218>. Acesso em: 5 de março de 2024.

GRECO, Leonardo. Garantias fundamentais do processo: o processo justo. **Novos Estudos Jurídicos** – Ano VII, n. 14, p. 09-68, abril/2008.

MARTINS, Leonardo. **Tribunal Constitucional Federal Alemão**: decisões anotadas sobre direitos fundamentais. Volume 1. São Paulo: Fundação Konrad-Adenauerv Stiftung 2016.

MARTINS JÚNIOR, Wallace Paiva. **Transparência Administrativa**: publicidade, motivação e participação popular. 2. ed. São Paulo: Saraiva, 2010.

MENDES, Laura Schertel F. Autodeterminação Informativa: a história de um conceito. **Revista Pensar**. Fortaleza, v. 25, n. 4, p.1-18, out./dez. 2020.

MENDES, Laura Schertel F. O Supremo Tribunal Federal e a proteção constitucional dos dados pessoais: rumo a um Direito Fundamental autônomo. *In* DONEDA, Danilo (*et al*.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: 2021.

PALHARES, Felipe. Cookies: contornos atuais. *In* PALHARES, Felipe (Coord.). **Temas Atuais de Proteção de Dados**. São Paulo: Thonson Reuters, 2020.

QUEIROZ, Rafael Mafei R. Direito à privacidade e proteção de dados pessoais: aproximações e distinções. **Revista do Advogado** 2019 v. 39 n. 144 nov, pp. 15-21.

RODOTÀ, Stefano. **A vida na sociedade da vigilância privada hoje**. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar. 2008.

SOLOVE, Daniel J. **The digital person**: technology and privacy in the information age. New York University Press: New York, 2004.

SOLOVE, Daniel J. "Privicy Self-management and the Consent Dilemma". **Harvard Law Review**, vol. 126, p. 1880-1993, 2013.

SCHWARTZ, Paul. The Computer in German and American Constitucional Law. **American Journal of Comparative Law***, 37*, 675-705, 1989.

WARREN, Samuel; BRANDEIS, Louis. "The Right to Privacy". in **Harvard Law Review** 193, vol. IV, 1890.

WACKS, Raymond. **Personal Information**: Privacy and the Law. Oxford: Clarendon Press, 1989.

WESTIN, Alan. **Privacy and freedom**. New York: Atheneum, 1967.

ZANINI, Leonardo E. A. O surgimento e o desenvolvimento do right of privacy nos Estados Unidos. **Revista Brasileira de Direito Civil – RBDCivil** – Volume 3 – jan/mar 2015.