

**INSTITUTO BRASILEIRO DE ENSINO, DESENVOLVIMENTO E PESQUISA**  
**PROGRAMA DE PÓS-GRADUAÇÃO *STRICTO SENSU* EM DIREITO**  
**DOUTORADO EM DIREITO CONSTITUCIONAL**

RENATO DA COSTA LINO DE GÓES BARROS

**O PRINCÍPIO DA PUBLICIDADE E A DEFINIÇÃO DE PARÂMETROS GERAIS**  
**DE RESTRIÇÃO DE ACESSO A DADOS PESSOAIS EM PROCESSOS JUDICIAIS**  
**ELETRÔNICOS PARA PROTEÇÃO DE DADOS**

**BRASÍLIA**

**2024**

RENATO DA COSTA LINO DE GÓES BARROS

**O PRINCÍPIO DA PUBLICIDADE E A DEFINIÇÃO DE PARÂMETROS GERAIS  
DE RESTRIÇÃO DE ACESSO A DADOS PESSOAIS EM PROCESSOS JUDICIAIS  
ELETRÔNICOS PARA PROTEÇÃO DE DADOS**

Tese de Doutorado desenvolvida sob a orientação do Prof. Dr. Nelson Rosenthal e apresentada ao PPGD/IDP como requisito parcial para a obtenção do título de Doutor em Direito Constitucional, na linha de pesquisa “Direito Privado e Processual na Ordem Constitucional”.

**BRASÍLIA**

**2024**

## Código de catalogação na publicação – CIP

B277p Barros, Renato da Costa Lino de Góes  
O Princípio da Publicidade e a definição de parâmetros gerais de restrição de acesso a dados pessoais em processos judiciais eletrônicos para proteção de dados. / Renato da Costa Lino de Góes Barros. — Brasília: Instituto Brasileiro Ensino, Desenvolvimento e Pesquisa, 2024.

117 f .

Tese — Instituto Brasileiro Ensino, Desenvolvimento e Pesquisa – IDP, Doutorado Acadêmico em Direito Constitucional, 2024.

Orientador: Prof. Dr. Nelson Rosenthal

1. Publicidade. 2. Proteção de dados. 3. Restrição de Acesso. I.Título

CDDir 341.2

RENATO DA COSTA LINO DE GÓES BARROS

**O PRINCÍPIO DA PUBLICIDADE E A DEFINIÇÃO DE PARÂMETROS GERAIS  
DE RESTRIÇÃO DE ACESSO A DADOS PESSOAIS EM PROCESSOS JUDICIAIS  
ELETRÔNICOS PARA PROTEÇÃO DE DADOS**

Tese de Doutorado desenvolvida sob a orientação do Prof. Dr. Nelson Rosenvald e apresentada ao PPGD/IDP como requisito parcial para a obtenção do título de Doutor em Direito Constitucional, na linha de pesquisa “Direito Privado e Processual na Ordem Constitucional”.

Brasília, 13 de junho de 2024

**BANCA EXAMINADORA**

---

**Prof. Dr. Nelson Rosenvald**  
**Orientador**

Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa

---

**Prof. Dr. Ademar Borges de Sousa Filho**

Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa  
Membro Interno

---

**Prof. Dr. Rodolfo Mário Veiga Pamplona Filho**

Universidade Federal da Bahia  
Membro Externo

---

**Prof. Dr. João Victor Rozatti Longhi**

Universidade Estadual do Norte do Paraná  
Membro Externo

Ao meu pai, meu maior exemplo, com minhas  
saudades eternas.

## **AGRADECIMENTOS**

Agradeço à minha Mari e aos meus filhos, Renato e João Bernardo, amores da minha vida, por toda compreensão, dedicação e apoio no curso deste Doutorado.

Aos meus pais por todos os esforços e dedicação para que eu pudesse ter uma boa formação.

Ao meu orientador, Dr. Nelson Rosenvald, por todo o apoio, gentileza e dedicação no curso da orientação do meu trabalho.

Aos meus mestres, em especial ao Dr. Rodolfo Pamplona, por todo auxílio e lições ao longo da minha caminhada acadêmica.

Aos amigos do JCL, em especial a Pedro e Leonardo Telles, por todo o carinho, apoio e incentivo.

Aos demais familiares, amigos e pessoas que me querem bem. A todos vocês minha eterna gratidão!

“[...] Desse modo, a afirmação da força normativa do direito fundamental à proteção de dados pessoais decorre da necessidade indissociável de proteção à dignidade da pessoa humana ante a contínua exposição dos indivíduos aos riscos de comprometimento da autodeterminação informacional nas sociedades contemporâneas”.

Min. Gilmar Mendes (julgamento da ADI n. 6.390, referente à MP954).

## RESUMO

A tese demonstrou que a publicidade dos atos processuais é uma garantia processual, que possibilita o controle dos atos judiciais por terceiros e desestimula julgamentos arbitrários. O ordenamento jurídico brasileiro prevê hipóteses em que a publicidade é relativizada, para defesa da privacidade ou quando o interesse social assim o exigir. Diante da institucionalização do processo eletrônico no país e da ausência de normas efetivas que garantam a restrição de acesso a dados que não tenham interesse público, os dados pessoais constantes nos processos que não tramitam em segredo de justiça estão expostos e vulneráveis a um tratamento ilegítimo, conforme revela o tema 1141 do Supremo Tribunal Federal. A tese evidenciou que é possível a limitação de acesso às informações constantes em atos processuais para a preservação dos dados pessoais em nome do livre desenvolvimento da personalidade, sem que se viole a garantia constitucional à publicidade. Neste sentido, foram definidos parâmetros gerais de restrição de acesso a informações pessoais em atos processuais para proteção de dados. Dentro da classificação sugerida, foram classificados os dados pessoais contidos em um processo judicial em três tipos, quais sejam, dados pessoais não relacionados à causa de pedir, dados pessoais relacionados à causa de pedir e dados pessoais sensíveis e íntimos. A proposta consiste na instituição de um sigilo seletivo e extraprocessual de dados pessoais que não têm interesse público e a decretação de segredo de justiça em processos, cuja causa de pedir envolva dados sensíveis e íntimos. Os demais dados, de interesse público, não sofreriam limitações de acesso, sendo o mínimo necessário para a compreensão da lide.

**Palavras-chave:** Publicidade; Proteção de dados; Restrição de Acesso; Dados Processuais.



## ABSTRACT

The thesis demonstrated that the publicity of procedural acts is a procedural guarantee, which enables control of judicial acts by third parties and discourages arbitrary judgments. The Brazilian legal system provides for hypotheses in which advertising is relativized, to protect privacy or when social interests so require. Given the institutionalization of the electronic process in the country and the absence of effective standards that guarantee the restriction of Access to data that are not of public interest, personal data contained in processes that are not processed under judicial secrecy are exposed and vulnerable to illegitimate treatment, as revealed in theme 1141 of the Federal Supreme Court. The thesis showed that it is possible to limit Access to information contained in procedural acts to preserve personal data in the name of the free development of personality, without violating the constitutional guarantee to publicity. In this sense, general parameters for restricting Access to personal information in procedural acts for data protection were redefined. Within the proposed classification, personal data contained in a judicial process were classified into three types, namely, personal data not related to the cause of action, personal data related to the cause of action and sensitive and intimate personal data. The proposal consists of the establishment of selective and extra-procedural secrecy of personal data that is not of public interest and the decree of judicial secrecy in processes whose cause of action involves sensitive and intimate data. Other data, of public interest, would not suffer Access limitations, being the minimum necessary to understand the dispute.

**Keywords:** Advertising; Data protection; Access Restriction; Procedural Data.

**LISTA DE ABREVIATURAS E SIGLAS**

AB2L	Associação Brasileira de Lawtechs e Legaltechs
ABRAJI	Associação Brasileira de Jornalismo Investigativo
CLT	Consolidação das Leis Trabalhistas
CC	Código Civil
CDC	Código de Defesa do Consumidor
CPC	Código de Processo Civil
CF	Constituição Federal de 1988
CJF	Conselho da Justiça Federal
CNJ	Conselho Nacional de Justiça
CSJT	Conselho Superior da Justiça do Trabalho
GDPR	General Data Protection Regulation
IBGE	Instituto Brasileiro de Geografia e Estatística
IRDR	Incidente de Resolução de Damandas Repetitivas
IRIS	Instituto de Referência em Internet e Sociedade
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados
NTCI	Novas Tecnologias de Comunicação e de Informação
OAB	Ordem dos Advogados do Brasil
OKBR	Open Knowledge Brasil
PNAD	Pesquisa Nacional por Amostra de Domicílios
RGPD	Regulamento Geral sobre a Proteção de Dados
STF	Supremo Tribunal Federal
TRT	Tribunal Regional do Trabalho
TST	Tribunal Superior do Trabalho

## SUMÁRIO

<b>INTRODUÇÃO</b> .....	12
<b>1. O PRINCÍPIO DA PUBLICIDADE DOS ATOS PROCESSUAIS</b> .....	17
1.1 A IMPORTÂNCIA DO PRINCÍPIO NO ESTADO DEMOCRÁTICO DE DIREITO.....	17
1.2 AS RESOLUÇÕES N. 121 DO CONSELHO NACIONAL DE JUSTIÇA E N. 139 DO CONSELHO SUPERIOR DA JUSTIÇA DO TRABALHO: A DIVULGAÇÃO DE DADOS PROCESSUAIS ELETRÔNICOS NA REDE MUNDIAL DE COMPUTADORES.....	25
1.3 OS PROCESSOS EM SEGREDO DE JUSTIÇA .....	31
<b>2. O DIREITO FUNDAMENTAL A PRIVACIDADE, A INTIMIDADE, A AUTODETERMINAÇÃO INFORMATIVA E A PROTEÇÃO DE DADOS</b> .....	39
2.1 A EXTENSÃO DA PRIVACIDADE, DA INTIMIDADE E DA AUTODETERMINAÇÃO INFORMATIVA.....	39
2.2 O DIREITO FUNDAMENTAL A PROTEÇÃO DE DADOS: O RECONHECIMENTO PELO SUPREMO TRIBUNAL FEDERAL.....	44
2.2.1 Noções gerais sobre a materialidade dos direitos fundamentais.....	44
2.2.2 A Medida Provisória n. 954/2020 e o julgamento pelo STF.....	48
2.3 A LEI GERAL DE PROTEÇÃO DE DADOS.....	58
2.4 OS DADOS PESSOAIS E OS DADOS PESSOAIS SENSÍVEIS.....	61
<b>3. A PROTEÇÃO DE DADOS PESSOAIS NO PROCESSO JUDICIAL QUE NÃO TRAMITA EM SEGREDO DE JUSTIÇA</b> .....	70
3.1 O ACESSO AOS AUTOS PROCESSUAIS E OS DADOS PESSOAIS CONSTANTES NA INICIAL.....	70
3.2 O CRUZAMENTO DE DADOS: A DIVULGAÇÃO POR PROVEDOR DE APLICAÇÕES DE INTERNET DE CONTEÚDOS DE PROCESSOS JUDICIAIS - O TEMA 1141 DO SUPREMO TRIBUNAL FEDERAL.....	77
3.3 A AFETAÇÃO A AUTODETERMINAÇÃO EM DECORRÊNCIA DE INTERESSE PÚBLICO E MEDIANTE DEFINIÇÃO DE REGRAS - O ACÓRDÃO 403.215 DO STJ DE PORTUGAL.....	90

3.4 A PUBLICIDADE DE ATOS DE PROCESSO COM PESSOAS COM INCAPACIDADE - O ACÓRDÃO 720.2022 DO STJ DE PORTUGAL.....	97
3.5 DEFINIÇÃO DE PARÂMETROS GERAIS DE RESTRIÇÃO DE ACESSO A DADOS PESSOAIS CONSTANTES NO PROCESSO JUDICIAL.....	105
3.6 A IMPORTÂNCIA DE IMPLANTAÇÃO E EXECUÇÃO DE UM PROGRAMA DE COMPLIANCE PARA EVITAR O VAZAMENTO DE DADOS.....	114
<b>CONCLUSÃO</b> .....	118
<b>REFERÊNCIAS</b> .....	121

## INTRODUÇÃO

A publicidade de atos processuais é uma garantia processual concedida às partes, assim como atende aos interesses de terceiros. Trata-se de um princípio fundamental para a sustentação do Estado Democrática de Direito.

Visa-se, com a publicização dos atos processuais, garantir o direito à informação, desestimulando julgamentos arbitrários e possibilitando o controle dos atos judiciais por terceiros. A inobservância desta garantia processual implica, inclusive, nulidade do ato processual.

No entanto, a própria Constituição Federal, em seus artigos 5º, inciso LX e 93, IX, admite a restrição à publicidade de atos processuais para defesa da privacidade ou quando o interesse social assim o exigir, prevendo a possibilidade de sigilo do processo, com a determinação do segredo de justiça.

Neste particular, o Código de Processo Civil disciplina as hipóteses de segredo de justiça expressamente garantidas.

Já a Lei n. 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), que disciplina a proteção de dados no Brasil, salvaguarda os dados pessoais e elenca a proteção à privacidade, à inviolabilidade da intimidade e à autodeterminação informativa, como fundamentos para a proteção de dados pessoais.

A digitalização de processos no país agravou a situação de vulnerabilidade dos dados pessoais constantes nos processos judiciais, que estão expostos à coleta e ao tratamento indevidos.

Como se verá, existem sistemas avançados que, por cruzamento de dados, conseguem realizar a coleta e tratar dados de uma forma diferente do que os próprios órgãos públicos divulgadores da informação realizam.

O tema proposto é atual diante das repercussões trazidas com a vigência da LGPD no Brasil, possui elevado impacto social e interessa a todos que, de alguma forma, valem-se de

processos judiciais para atingir determinada pretensão. Afinal, em um processo judicial, é possível acessar uma série de dados pessoais das partes envolvidas.

A título de exemplo, em uma petição inicial, podem conter dados de qualificação das partes, a exemplo de nome, nacionalidade, estado civil, profissão, inscrição no registro civil e no cadastro de pessoas físicas, além de filiação, e-mail e telefone, que poderão ser utilizados indevidamente.

Muitas vezes, a inicial também é acompanhada de documentos pessoais, como a cédula de identidade, que poderão ser reproduzidos e utilizados por terceiros.

Ainda, a petição inicial pode revelar dados sensíveis, a exemplo da opção religiosa e orientação sexual ou, até mesmo, do estado de saúde de um dos envolvidos, de modo que esses dados poderão ser utilizados indevidamente, inclusive, como forma de discriminação.

Destaca-se também que, nos processos digitais, a vulnerabilidade dos dados é ainda maior e mais grave, já que é possível fazer o *download* com as cópias dos autos, gerando arquivo que terá circulação livre e indistinta, sem que haja qualquer controle e a possibilidade de rastrear quem gerou o arquivo.

Para que se possa combater esta situação, é necessário compreender a extensão atual dos conceitos da publicidade, privacidade, autodeterminação informativa e proteção de dados, de forma que se proponham limites para salvaguardar os dados pessoais constantes nos processos judiciais, que são bens de valor imaterial e que são atributos da personalidade.

No cenário atual, não há outra opção senão disponibilizar os dados pessoais no momento da propositura da ação, assim como não há hipótese legalmente instituída para, ao menos, garantir um sigilo seletivo e a não propagação destes dados pessoais.

Nesse sentido, uma reflexão acerca de uma eventual limitação de acesso às informações constantes no processo judicial é imprescindível para a preservação dos dados pessoais, especialmente diante do reconhecimento ao direito fundamental à proteção de dados, sem que se viole a garantia constitucional à publicidade para o convívio pleno entre os princípios e regras vigentes.

Nesta linha, define-se o seguinte problema de pesquisa: É possível a limitação de acesso aos dados pessoais constante no processo judicial em nome do direito fundamental à proteção

de dados, à privacidade, à intimidade e à autodeterminação informativa, sem que se viole a garantia constitucional à publicidade?

O objetivo geral desta pesquisa é, então, definir se seria possível estabelecer limites ao princípio da publicidade neste enfoque e, eventualmente, especificá-los em nome da proteção de dados pessoais.

Para tanto, pretende-se: a) identificar a interpretação atual e adequada dos conceitos relacionados à publicidade, à privacidade, à intimidade e à autodeterminação informativa, com base no ordenamento jurídico vigente; b) compreender a extensão atual do direito à proteção de dados, sob a luz da lei geral de proteção de dados; c) definir a natureza jurídica dos dados pessoais, que são bens de valor imaterial e que são atributos da personalidade; d) traçar quais seriam os dados pessoais que poderiam ser salvaguardados e quais seriam os limites e os meios para uma proteção efetiva neste contexto atual.

A metodologia utilizada para responder à pergunta central é prioritariamente a pesquisa bibliográfica. Assim, um extenso levantamento da bibliografia relacionada ao tema foi realizado, por meio da seleção de artigos científicos selecionados nas plataformas Portal Periódicos da CAPES e Scientific Electronic Library Online (SciELO), além de livros, dissertações e teses, no intuito de identificar as reflexões da doutrina que possam contribuir com a pesquisa.

Posteriormente, foi realizada uma pesquisa documental, com foco na jurisprudência, com análise de leis, precedentes nacionais e estrangeiros, assim como temas recentes de repercussão geral ainda pendentes de julgamentos pelos tribunais superiores.

Cabe ressaltar que, segundo Lakatos e Marconi (2010), na pesquisa documental a fonte da coleta de dados se refere a documentos, escritos ou não, constituindo o que se denomina de fontes primárias, a exemplo de contratos e publicações administrativas e parlamentares.

Buscando atingir os objetivos estabelecidos, esta tese está estruturada em três capítulos.

No Capítulo 1, pretende-se analisar o princípio da publicidade, partindo da importância do referido princípio no Estado Democrático de Direito.

Em seguida, serão analisadas a Resolução n. 121, do Conselho Nacional de Justiça, e a n. 139, do Conselho Superior da Justiça do Trabalho, que são normas regulamentadoras e

marcos normativos sobre a divulgação de dados processuais eletrônicos na rede mundial de computadores.

Ademais, ainda neste primeiro capítulo serão abordados os processos em segredo de justiça, com ênfase nas hipóteses legalmente previstas.

O Capítulo 2 será dedicado aos direitos fundamentais à privacidade, intimidade, autodeterminação informativa e proteção de dados, sendo feita uma análise sobre a extensão desses direitos, assim como um exame acerca da Lei Geral de Proteção de Dados (LGPD).

Também serão analisados os conceitos sobre os dados pessoais e os dados pessoais sensíveis, apontando as razões para a sua diferenciação e os aspectos relevantes acerca da sua tutela.

Será feita uma análise de como se deu – no Brasil – o reconhecimento da autodeterminação informativa e da proteção de dados no sistema normativo como direitos fundamentais, fazendo uma análise dos fundamentos apresentados no julgamento das ADINS, propostas contra a Medida Provisória de n. 954/2020 pelo Supremo Tribunal Federal (STF).

O Capítulo 3 será dedicado ao tema de proteção de dados no processo judicial que não tramita em segredo de justiça.

Analisar-se-á, inicialmente, a questão sobre o acesso aos autos processuais e se fará uma reflexão sobre os dados pessoais constantes nos processos judiciais e a importância de sua preservação.

O referido capítulo trata acerca do tema 1141 do STF, que se refere ao cruzamento de dados decorrente da divulgação por provedor de aplicações de internet de conteúdos de processos judiciais, evidenciando aspectos destacados no caso.

Será feita, ainda, uma análise sobre a afetação e a autodeterminação em decorrência de interesse público e mediante a definição de regras, assim como uma análise sobre a publicidade de atos de processo que envolvam pessoas com algum tipo de incapacidade, sendo que ambas as análises partirão de precedentes oriundos de tribunal estrangeiro, a saber, o Supremo Tribunal de Justiça de Portugal.



Com base nestes casos, buscar-se-á definir parâmetros gerais de restrição de acesso a informações pessoais constantes nos processos judiciais para proteção de dados. Definidas as premissas e estabelecidos os parâmetros, será feita uma análise sobre a necessidade e conveniência da adoção de medidas para evitar inconsistências, inclusive, no que se refere a um programa de *compliance*.

## 1. O PRINCÍPIO DA PUBLICIDADE DOS ATOS PROCESSUAIS

### 1.1 A IMPORTÂNCIA DO PRINCÍPIO NO ESTADO DEMOCRÁTICO DE DIREITO

A Constituição Federal Brasileira de 1988 prevê a publicidade geral dos atos processuais, somente admitindo a sua restrição quando a defesa da intimidade ou o interesse social o exigirem.

É isso o que dispõe o inciso LX do artigo 5º da CF:

Art. 5º 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; [...]. (BRASIL, 1988).

Mas não é só. A Constituição Federal, nos incisos IX e X do artigo 93, prevê também que:

Art. 93. 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;

X - as decisões administrativas dos tribunais serão motivadas e em sessão pública, sendo as disciplinares tomadas pelo voto da maioria absoluta de seus membros; [...]. (BRASIL, 1988).

Sobre a constitucionalização do princípio da publicidade dos atos processuais, critica José Afonso da Silva (2006, p. 156):

A publicidade dos atos do Poder Judiciário está especialmente prevista no art. 93, IX, de tal sorte que a previsão do inciso ora em comentário a reforça e indica quando é possível admitir os chamados “atos processuais em segredo de justiça”. A legislação processual sempre consignou o princípio da publicidade de atos processuais. Isso

nunca constituiu um problema, para que fosse necessário transformá-lo em norma constitucional.

Independentemente da crítica de parte da doutrina, o princípio da publicidade dos atos processuais encontra-se expressamente previsto na Constituição Federal e irradia seus efeitos nas normas infraconstitucionais.

Os artigos 8º e 11º do Código de Processo Civil (CPC) preveem, respectivamente, que “ao aplicar o ordenamento jurídico, o juiz atenderá aos fins sociais e às exigências do bem comum, resguardando e promovendo a dignidade da pessoa humana e observando a proporcionalidade, a razoabilidade, a legalidade, a publicidade e a eficiência” e “todos os julgamentos dos órgãos do Poder Judiciário serão públicos, e fundamentadas todas as decisões, sob pena de nulidade” (BRASIL, 2015).

Por meio da publicidade dos atos processuais, pretende-se ter meios para o controle do exercício jurisdicional estatal, evitando-se, por meio deste, a existência de julgamentos secretos.

Neste sentido, excepcionalmente, é admitida a restrição de acesso em relação a terceiros, por razões listadas expressamente em lei.

Em relação às partes litigantes, em princípio, não existiria uma norma que amparasse a restrição de acesso direcionada especificamente à parte contrária. Isto porque, em nome do contraditório e da ampla defesa, as partes precisam ter acesso a todas as informações constantes nos autos.

O princípio da publicidade dos atos processuais permite também que haja um controle de opinião pública sobre a prestação jurisdicional, garantido pela motivação dos atos judiciais.

Neste sentido, pontua Fredie Didier Jr (2022, p. 130) que:

Os atos processuais não de ser públicos. O princípio da publicidade gera o direito fundamental à publicidade. Trata-se de direito fundamental que tem, basicamente, duas funções: a) proteger as partes contra juízos arbitrários e secretos (e, nesse sentido, é conteúdo do devido processo legal, como instrumento a favor da imparcialidade e independência do órgão jurisdicional); b) permitir o controle da opinião pública sobre os serviços de justiça, principalmente sobre o exercício da atividade jurisdicional.

Ademais, sobre a consolidação do princípio da publicidade e diferenciação das vertentes interna e externa da publicidade dos atos processuais, pontua Rocha (2017, p. 277):

A norma, como não poderia deixar de ser, visa à garantia da publicidade de todo e qualquer ato processual. Trata-se de prerrogativa do cidadão para fins de controle do exercício do poder estatal, impedindo assim a ocorrência de julgamentos secretos e arbitrários. Afinal, incabível se falar em devido processo legal sem ciência das partes – e não só delas, mas de todo e qualquer cidadão – dos atos praticados no processo, principalmente pelos próprios órgãos do Poder Judiciário, no exercício de sua função jurisdicional. Evidente, no entanto, existirem exceções à norma, conforme se extrai da própria redação do art. 5º, LX, da Constituição Federal, o qual dispõe que “a lei só poderá restringir a publicidade dos atos processuais quando a defesa da intimidade ou o interesse social o exigirem”. Há que se deixar claro, por outro lado, que a publicidade dos atos jamais poderá ser reduzida a tal ponto de impedir o seu conhecimento pelas próprias partes do processo ou seus advogados: trata-se da dimensão interna da publicidade, garantia mínima dos jurisdicionados com vistas a impedir julgamentos secretos. Somente a publicidade externa – ou seja, perante terceiros –, portanto, pode ser restringida.

A publicidade dos atos processuais também deve ser entendida como uma verdadeira garantia à democracia.

O amplo acesso à informações é uma premissa do Estado Democrático de Direito, assim como reflete a transparência necessária e esperada da Administração Pública, conforme previsto no art. 37 da Constituição Federal.

Ademais, a possibilidade de se ter acesso aos elementos dos autos, que revelam as condições em que uma determinada decisão foi tomada, mostra-se fundamental para a compreensão acerca da correta aplicação do ordenamento jurídico que sustenta o Estado Democrático de Direito.

Sobre o tema, ponderam Andrade e Maranhão (2021, p. 2):

Pela primeira deontológica, argumenta-se que a publicidade é indispensável à democracia, uma vez que o cidadão somente pode exercer seus direitos políticos se tiver informações suficientes sobre a atividade estatal. A publicidade se confunde aqui com a "dimensão informacional" da democracia, do "regime de poder visível", conforme citadíssima passagem de Norberto Bobbio. Já como técnica administrativa, a publicidade é apenas um meio voltado para consecução de certas finalidades concretas almejadas pela Administração. Trata-se da "transparência", propagada como uma "cura" para a corrupção e o abuso de autoridade. Fala-se, inclusive, em tipos diferentes de transparência (ativa, passiva, política de dados abertos, transparência horizontal, transparência vertical, etc.) de que pode lançar mão o administrador para atingir seu fim. Essas duas abordagens (deontológica e consequencialista) são, em realidade, complementares a depender da análise a ser feita. No controle de constitucionalidade, por exemplo, a publicidade é concebida como um valor essencial à democracia. Por outro lado, ao se desenhar a política de dados de um órgão administrativo, a publicidade deve ser vista como técnica. Deve-se pensar qual o objetivo a atingir (controle democrático, aumento de eficiência, proteção de interesses de terceiros), quais os tipos de informações necessárias, qual o

modo, passivo ou ativo, para conferir acesso, e qual a maneira mais econômica de se disponibilizar os dados etc.

Com a publicização dos atos processuais, garante-se o direito à informação e a possibilidade de controle dos atos judiciais.

Em processos que não estão em regime de segredo de justiça, o sistema garante a todos o direito de requerer certidões, consultar os autos e assistir audiências, obtendo todas as informações necessárias para este controle.

A intenção do ordenamento jurídico é evidente: viabilizar que os atos sejam fiscalizados e que seja garantida a imparcialidade esperada nas decisões judiciais, desestimulando arbitrariedades, num ambiente de transparência e de amplo acesso a informações.

Neste sentido, o STF, por meio do voto do Ministro Celso de Melo, no Agravo Regimental no HC 119.538/SP, julgado em 22/10/2013 pela Segunda Turma, em que se julgou ação penal que envolve descumprimento da obrigação de pagamento de alimentos, assim se posicionou ao indeferir o requerimento de decretação ao segredo de justiça:

[...] De outro lado, quanto ao pedido de decretação de sigilo, tenho para mim que não justifica o acolhimento deste pleito, eis que o “segredo de justiça”, em caso de alimentos, somente se legitima em face do respectivo processo de natureza civil (CPC, art. 155, II). No caso, trata-se de ação penal de “habeas corpus”, onde se controverte em torno do “jus libertatis” do devedor alimentante, valendo destacar, ainda, que a decretação do regime de sigilo assume caráter absolutamente excepcional, considerado o que dispõe a própria Constituição da República, no inciso IX do art. 93. Nada deve justificar, em princípio, a tramitação, em regime de sigilo, de qualquer procedimento que tenha curso em juízo, pois, na matéria, deve prevalecer, ordinariamente, a cláusula de publicidade. Não custa rememorar, tal como sempre tenho assinalado nesta Suprema Corte, que os estatutos do poder, numa República fundada em bases democráticas, não podem privilegiar o mistério. Na realidade, a Carta Federal, ao proclamar os direitos e deveres individuais e coletivos (art 5º), enunciou preceitos básicos cuja compreensão é essencial à caracterização da ordem democrática como um regime do poder visível, ou, na expressiva lição de NORBERTO BOBBIO (“O Futuro da Democracia”, p. 86, 1986, Paz e Terra), como “modelo ideal do governo público em público”. A Assembleia Nacional Constituinte, em momento de feliz inspiração, repudiou o compromisso do Estado com o mistério e com o sigilo, tão fortemente realçados sob a égide autoritária do regime político anterior. Ao dessacralizar o segredo, a Assembleia Constituinte restaurou velho dogma republicano e expôs o Estado, em plenitude, ao princípio democrático da publicidade, convertido, em sua expressão concreta, em fator de legitimação das decisões e dos atos governamentais. Isso significa, portanto, que somente em caráter excepcional os procedimentos penais poderão ser submetidos ao (impropriamente denominado) regime de sigilo (“rectius”: de publicidade restrita), não devendo tal medida converter-se, por isso mesmo, em prática processual ordinária, sob pena de deslegitimação dos atos a serem realizados no âmbito da causa penal. É por tal razão que o Supremo Tribunal Federal tem conferido visibilidade a procedimentos penais

originários em que figuram, como acusados ou como réus, os próprios membros do Poder Judiciário (como sucedeu, p. ex., no Inq 2.033/DF e no Inq. 2.424/DF), pois os magistrados, também eles, como convém a uma República fundada em bases democráticas, não dispõem de privilégios nem possuem gama mais extensa de direitos e garantias que os outorgados, em sede de persecução penal, aos cidadãos em geral. Essa orientação nada mais reflete senão a fidelidade desta Corte Suprema às premissas que dão consistência doutrinária, que imprimem significação ética e que conferem substância política ao princípio republicado, que se revela essencialmente incompatível com tratamentos diferenciados, fundados em ideações e práticas de poder que exaltam, sem razão e sem qualquer suporte constitucional legitimador, o privilégio pessoal e que desconsideram, por isso mesmo, um valor fundamental à própria configuração da ideia republicana que se orienta pelo vetor axiológico da igualdade. [...] (BRASIL, 2013).

Observa-se, por meio dos seus fundamentos, o entendimento do Supremo Tribunal Federal sobre a excepcionalidade das hipóteses de decretação de sigilo e sobre o prestígio da publicidade, que veio estampada na Constituição Federal de 1988, em detrimento do mistério e do sigilo que eram marcas de um período que antecedeu a nova ordem constitucional brasileira.

No entendimento do STF, o “mistério” e o “segredo” seriam incompatíveis com os preceitos democráticos e tornariam “ilegítimas” as decisões.

Assim, uma função pessoal exercida pelo litigante não justificaria uma restrição e poderia causar uma violação à igualdade, também prestigiada pela Constituição Federal do Brasil. Com a ampla publicidade dos atos processuais prestigia-se, também, a isonomia e a imparcialidade, outros valores inerentes à democracia e ao Estado Democrático de Direito.

Ademais, vale destacar que o Brasil adotou o sistema de precedentes obrigatórios, o que torna ainda mais evidente a importância da publicidade dos atos processuais diante da necessidade de analisar os precedentes, sendo que o parágrafo 5º do artigo 927 do CPC prevê que “os tribunais darão publicidade a seus precedentes, organizando-os por questão jurídica decidida e divulgando-os, preferencialmente, na rede mundial de computadores” (BRASIL, 2015).

Uma iniciativa diferenciada adotada no Brasil, e que tem relação com o princípio da publicidade dos atos processuais, é a transmissão, em tempo real, dos julgamentos proferidos pelo STF. Por meio destes é possível acompanhar o posicionamento de cada ministro a respeito de cada tema e o debate de ideias para o firmamento de determinado entendimento pelas turmas ou pelo plenário do Supremo.

Trata-se de iniciativa que demanda atenção e cuidado em relação à imagem da Corte Suprema, especialmente nos casos em que o debate de ideias é desvirtuado por

desentendimentos e desavenças pessoais entre os ministros. Em que pese não esteja no recorte definido neste estudo, é importante ressaltar que, nestas transmissões, haja também o cuidado de se divulgar apenas as informações pessoais estritamente necessárias à compreensão da causa em nome da proteção de dados.

Afinal, neste ambiente de publicidade geral<sup>1</sup> - e não restrita -, dados pessoais constantes nos processos judiciais tornam-se vulneráveis, possibilitando a ocorrência de situações prejudiciais para as partes, que depositam inúmeras informações pessoais no processo.

Como se verá em tópico específico, por meio dos sites dos tribunais, dos bancos de dados de decisões e da análise de publicação por meio do Diário Eletrônico, é possível se obter amplo acesso às informações de processos judiciais.

A vulnerabilidade dos dados nos autos processuais se tornou mais grave com a implementação dos processos digitais – realidade já consolidada do judiciário brasileiro e regulamentada por meio da Lei 11.419, de 2006, em que não é possível o exercício eficiente acerca do controle de acesso aos documentos constantes nos autos processuais, especialmente quando se permite fazer facilmente cópias dos autos digitais, com a circulação livre e indistinta destes arquivos.

Diante deste cenário, é crescente a preocupação sobre a publicidade ampla dos autos digitais, já tendo sido aventada a possibilidade de relativização da publicidade e a restrição parcial de acesso.

Neste caminho, destaca Rocha (2017, p. 278) que:

---

<sup>1</sup> No relatório da análise realizada sobre o tratamento de dados pessoais na consulta de jurisprudência, pontuou o CNJ (2021, p. 7) que: “Com efeito, não se pode ignorar que, diferentemente do que ocorre em outros países, a publicidade de sessões de julgamento, de decisões judiciais e de demais atos processuais no sistema judicial brasileiro constitui uma longa tradição, reiteradamente reafirmada pelo Supremo Tribunal Federal: 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 disposição normativa que determine abstratamente segredo de justiça em todos os processos em curso perante Vara Criminal. (ADI 4.414/AL, Tribunal Pleno, Rel. Min. Luiz Fux, DJe n. 114, 17 jun. 2013). [...] a falta de formalização do acórdão, com base em norma regimental, configura ato atentatório à garantia constitucional da publicidade dos atos processuais. (RE 575.144/DF, Tribunal Pleno, Rel. Min. Ricardo Lewandowski, DJe n. 35, 20 fev. 2009) [São inconstitucionais] normas regimentais que, a pretexto de regulamentar o procedimento a ser seguido [...] para o julgamento penal de autoridades possuidoras de foro por prerrogativa de função, estabeleceram restrição ao direito fundamental da publicidade dos atos processuais, impondo a modalidade secreta de sessão [...]. (ADI 2.970/DF, Tribunal Pleno, Rel. Min. Ellen Gracie, DJ de 12 maio 2006)”.

De fato, antes mesmo da promulgação da Lei 11.419/2006 – e até da Constituição Federal de 1988 –, alguns estudiosos já alertavam para os riscos, na esfera processual, decorrentes dos rápidos avanços tecnológicos, que deixavam vulneráveis os sujeitos do processo, cuja privacidade poderia acabar exposta à coletividade. Propunha-se, assim, com base na redação do antigo art. 155 do CPC/1973 (LGL\1973\5), que, mesmo fora das hipóteses de segredo de justiça, o acesso aos autos do processo somente poderia ser facultado àquelas pessoas expressamente autorizadas, por lei, a consultá-los – caso, por exemplo, dos advogados em geral. Com o advento da Constituição Federal de 1988, no entanto, restou quase que unânime o entendimento segundo o qual, de acordo com o princípio da publicidade, todo e qualquer cidadão tem o direito de consultar os autos do processo, ainda que dele não seja parte, desde que não esteja submetido ao regime do segredo de justiça. O cenário mudou diante da implementação do processo digital. A partir da Lei 11.419/2006, e com a possibilidade de divulgação dos atos processuais na rede mundial de computadores, acessível por qualquer pessoa ao redor do mundo, muitos demonstraram preocupação com a publicidade excessiva dos autos digitais. Chegou-se a defender até mesmo a relativização do princípio processual da publicidade.

Na sequência, sobre a questão de restrição de acesso, Rocha (2017, p. 278) ainda pontua:

Na realidade, a própria Lei 11.419/2006 já traz disposições nesse sentido: em seu art. 11, § 6º, dispõe que “os documentos digitalizados juntados em processo eletrônico somente estarão disponíveis para acesso por meio da rede externa para suas respectivas partes processuais e para o Ministério Público, respeitado o disposto em lei para as situações de sigilo e de segredo de justiça.

Justamente por não ter sido admitida a relativização da publicidade processual, o referido dispositivo foi alterado por meio da Lei de n. 13.793, de 2019, passando a dispor que:

§ 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 (BRASIL, 2019).

A questão sobre o princípio da publicidade dos atos processuais e sobre a eventual institucionalização de restrições de acesso aos dados pessoais constantes nos atos processuais torna-se particularmente atual diante da vigência da Lei de n. 13.709 de 2018, LGPD, que disciplinou a questão da proteção de dados no país.

A problemática atual está agravada, pois, com os avanços tecnológicos, a publicidade dos atos processuais implica amplo acesso aos documentos processuais diante das facilidades decorrentes da digitalização por intermédio dos portais dos tribunais brasileiros.



Sobre esta questão, fazendo alusão a políticas de relativização de publicidade implementadas em outros países e citando exemplos que podem servir de referência para esta análise, pondera Cueva (2020, p. 204-205):

Na prática, a garantia constitucional de publicidade dos atos processuais, reproduzida nos estatutos processuais, acabou por se estender, em legislação especial, para os documentos constantes dos autos, que, com frequência, contem dados sensíveis. De fato, já se questiona se a publicidade no processo eletrônico deveria em alguma medida ser relativizada, em vista da enorme facilidade, proporcionada pelos meios tecnológicos à disposição de todos de obter e difundir informações sensíveis. Trata-se de antiga perquirição, que tem sido discutida também em outros países. Há mais de trinta anos, a Suprema Corte estadunidense, no caso *United States Department of Justice vs Reporters Committee for Freedom of the Press*, ao debater a lei federal de acesso à informação, não admitiu o acesso incondicionado às bases de dados do Federal Bureau of Investigation, à vista da enorme diferença entre obter informações à disposição do público em geral depois de proceder a cuidadosa busca em documentos em papel – sejam eles inquéritos policiais, autos judiciais, procedimentos administrativos encontrados em repartições públicas espalhadas por todo o país – e apertar algumas teclas de computador para, em pouco tempo, chegar a uma vasta gama de dados localizados em um único repositório de informação.

A adoção de medidas de restrição decorre de uma percepção no sentido de que, diante do estágio atual da tecnologia, em que se tem acesso às informações processuais por meio de arquivos digitalizados<sup>2</sup> e disponibilizados pelos portais dos órgãos judiciários brasileiros, é possível realizar o tratamento das informações, para incontáveis finalidades, com apenas “cliques” de qualquer lugar em que se esteja, obtendo um compilado de informações pessoais.

No caso das petições iniciais, são diversos os dados ali inseridos que estão vulneráveis a este tratamento não consentido, fugindo da finalidade inicialmente vinculada.

A título de exemplo, na petição inicial, são expostos dados pessoais relacionados à nacionalidade, profissão, estado civil, domicílio, números de registro civil e de inscrição no

---

<sup>2</sup> Sobre os desafios acerca da proteção de dados decorrentes da digitalização dos autos processuais, pontuam Bulzico e Sousa (2022, fls. 155): “Logo, no que diz a gestão incalculável de dados pelo poder Judiciário diante da expansiva utilização do Processo Judicial Eletrônico (PJe), o devido processo legal e a proteção aos dados pessoais conflitam em um ponto em comum: a publicidade. Neste artigo verificou-se que, para o exercício pleno do devido processo legal, de maneira orgânica, a publicidade é elemento indispensável; e, para a garantia da privacidade de dados pessoais das partes do processo, a publicidade deve ser a exceção e não a regra. Nesse ponto, conforme advertido por Marcelo Novelino, no Estado Democrático de Direito, os princípios, diferentemente das regras, devem ter aplicação mitigada quando verificada a contraposição. Considerando-se os princípios que balizam a Lei de Acesso à Informação, Política de Dados abertos, Controle Social e a Lei de Proteção de Dados Pessoais, é imprescindível observar o alcance a aplicação de cada um. Assim, partindo dessa análise de princípios em colisão, é preciso analisar as possibilidades de flexibilização de normas para adequar ao caso concreto, preservando a autonomia da vontade e informacional do titular dos dados”.

cadastro de pessoa física, como também são expostos – em muitas ocasiões – dados relacionados à intimidade.

Nos dias atuais, com a vigência da LGPD e o reconhecimento do direito fundamental à proteção de dados, é necessário impor parâmetros para a restrição de acesso a informações contidas nos processos judiciais, para adequação a esta nova realidade, o que será visto nos próximos capítulos.

## 1.2 AS RESOLUÇÕES N. 121 DO CONSELHO NACIONAL DE JUSTIÇA E N. 139 DO CONSELHO SUPERIOR DA JUSTIÇA DO TRABALHO: A DIVULGAÇÃO DE DADOS PROCESSUAIS ELETRÔNICOS NA REDE MUNDIAL DE COMPUTADORES.

O parágrafo 6º, do artigo 11, da Lei n. 11.419/2006, que dispõe sobre a informatização do processo civil, prevê que

[...] 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 tramitam em segredo de justiça (BRASIL, 2006).

A Resolução de número 121 do Conselho Nacional de Justiça<sup>3</sup>, de 5 de outubro de 2010 - alterada pelas Resoluções de números 137, datada de 13 de julho de 2011, e 143, datada de

---

<sup>3</sup> Sobre o CNJ, pontuam Oliveira e Silva (2023, p. 13) que: “O Conselho Nacional de Justiça (CNJ) foi criado pela Emenda Constitucional n. 45/2004 com o objetivo de efetuar o controle da atuação administrativa e financeira do Poder Judiciário e do cumprimento dos deveres funcionais dos juízes, cabendo-lhe, além de outras atribuições que lhe forem conferidas pelo Estatuto da Magistratura, desempenhar as atribuições previstas no art. 103-B da CR. Em sua resolução n. 121, de 05 de outubro de 2021, o CNJ estabelecia que a consulta aos dados básicos dos processos judiciais deveria disponibilizada na rede mundial de computadores (internet), assegurado o direito de acesso a informações processuais a toda e qualquer pessoa, independentemente de prévio cadastramento ou de demonstração de interesse, ressalvados os casos de sigilo ou segredo de justiça (art. 1º). Os dados de livre acesso seriam os seguintes: I – número, classe e assuntos do processo; II – nome das partes e de seus advogados; III – movimentação processual; e, IV – inteiro teor das decisões, sentenças, votos e acórdãos (art. 2º). O acesso ao inteiro teor do processo deveria ser assegurado ao advogado cadastrado e habilitado nos autos, as partes cadastradas e o membro do Ministério Público (art. 3º). E, posteriormente, em razão da promulgação da Lei n. 13.709/2018, que instituiu a Lei Geral de Proteção de Dados em nosso país, em 26 de abril de 2019, o CNJ, pela Portaria n. 63, instituiu um grupo de trabalho para elaborar estudos e propostas sobre a política de acesso às bases de dados dos



preservar o direito à intimidade, à vida privada, à autodeterminação informativa, à honra e à imagem das pessoas.

Sabe-se que a disponibilização, na rede mundial de computadores, de dados relativos aos processos judiciais pode gerar algum tipo de estigmatização em relação às partes em ações criminais, cíveis e trabalhistas, o que será analisado em capítulo próprio desta tese, com base no *Leading case* relacionado ao tema 1141 do STF.

Neste sentido, baseada no parágrafo sexto, do artigo 11º, da Lei 11.419 de 2006<sup>5</sup>, o sistema é concebido de forma a garantir que a consulta de dados básicos dos processos judiciais pela internet seja assegurada a toda e qualquer pessoa, independentemente de cadastro e de demonstração de interesse, com exceção daqueles processos que tramitam em segredo de justiça.

Nos termos do artigo 2º da mencionada resolução, os dados básicos de livre acesso são: “I – número, classe e assuntos do processo; II – nome das partes e de seus advogados; III – movimentação processual; IV – inteiro teor das decisões, sentenças, votos e acórdãos”.

Por sua vez, os advogados cadastrados e habilitados, as partes cadastradas e o membro do Ministério Público têm acesso a todo o conteúdo do processo eletrônico, conforme o artigo terceiro.<sup>6</sup>

Os sistemas de tramitação e acompanhamento processual eletrônico devem possibilitar ainda que “advogados, procuradores e membros do Ministério Público cadastrados”, que não

---

<sup>5</sup> “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 tramitem em segredo de justiça.

<sup>6</sup> A Resolução 185 de 2013 do CNJ, que instituiu o Sistema Processo Judicial Eletrônico – PJE como sistema de processamento de informações e prática de atos processuais prevê que: “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 tramitem 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. § 2º Os sítios eletrônicos do PJe dos Conselhos e dos Tribunais deverão ser acessíveis somente por meio de conexão segura HTTPS, e os servidores de rede deverão possuir certificados digitais Equipamento Servidor da ICP-Brasil adequados para essa finalidade.”

sejam vinculados a um determinado processo, possam acessar “automaticamente todos os atos e documentos processuais armazenados em meio eletrônico”.

Para tanto, eles devem demonstrar interesse, “para fins, apenas, de registro, salvo nos casos de processos em sigilo ou segredo de justiça”, devendo ficar registrado cada um destes acessos.

Sobre a extensão deste amplo e indiscriminado acesso, Doneda e Machado pontuam ainda que (2021, p. 347-348):

Quando se fala na proteção de informações, a preocupação única não pode ser a confidencialidade de dados, mas também a proteção da integridade e disponibilidade, todos estes os atributos da segurança de informação. Isso significa dizer que o poder público deve se preocupar com o acesso não autorizado das informações (proteção da confidencialidade) e também com sua integridade, ou seja, que não serão alteradas ou até mesmo eliminadas (proteção da disponibilidade) de forma deliberadamente não autorizada ou por erro.

A questão sobre a integridade de informações não é objeto deste estudo. A resolução ainda prevê, em seu artigo 4<sup>o</sup>, que as consultas públicas de acompanhamento disponíveis pela internet devem permitir a consulta pelo número atual ou número antigo, nomes das partes, número do cadastro do contribuinte perante o Ministério da Fazenda, nomes dos advogados, registro junto à Ordem dos Advogados do Brasil (OAB).

O referido artigo ainda prevê restrição de informações, nas consultas públicas dos sistemas de tramitação e acompanhamento processual dos Tribunais e Conselhos, nas seguintes hipóteses: (i) nos processos criminais, após o trânsito em julgado da decisão absolutória, da

---

<sup>7</sup> Dispõe o referido artigo que: “Art. 4.º As consultas públicas dos sistemas de tramitação e acompanhamento processual dos Tribunais e Conselhos, disponíveis na rede mundial de computadores, devem permitir a localização e identificação dos dados básicos de processo judicial segundo os seguintes critérios:

I – número atual ou anteriores, inclusive em outro juízo ou instâncias;

II – nomes das partes;

III – número de cadastro das partes no cadastro de contribuintes do Ministério da Fazenda;

IV – nomes dos advogados;

V – registro junto à Ordem dos Advogados do Brasil.

§ 1º. A consulta ficará restrita às seguintes situações: (Redação dada pela Resolução nº 143, de 30.11.2011)

I - ao inciso I da cabeça deste artigo, nos processo criminais, após o trânsito em julgado da decisão absolutória, da extinção da punibilidade ou do cumprimento da pena; (Redação dada pela Resolução nº 143, de 30.11.2011)

II - aos incisos I, IV e V da cabeça deste artigo, nos processo sujeitos à apreciação da Justiça do Trabalho. (Redação dada pela Resolução nº 143, de 30.11.2011) § 2º. Os nomes das vítimas não se incluem nos dados básicos dos processos criminais”.

extinção da punibilidade ou do cumprimento da pena, quando se limitará à disponibilização do “número atual ou anteriores, inclusive em outro juízo ou instâncias”; e (ii) no caso dos processos trabalhistas, as informações estariam restritas ao “número atual ou anteriores, inclusive em outro juízo ou instâncias”, aos “nomes dos advogados” e ao “registro junto à Ordem dos Advogados do Brasil”. Ademais, os nomes das vítimas não se incluem nos dados básicos dos processos criminais (BRASIL, 2010).

A resolução prevê, em seu art. 5.º, que a “disponibilização de consultas às bases de decisões judiciais impedirá, quando possível, a busca pelo nome das partes”, questão de elevada importância e que tem total ligação ao referido tema 1141 do STF, que será objeto de análise em tópico posterior deste estudo.

Em relação às certidões judiciais, a resolução disciplina que estas se prestam a identificar os termos circunstanciados, inquéritos e processos em que a pessoa a respeito figura no polo passivo e deve conter, nos termos do art. 7º: “I - nome completo; II – o número do cadastro de contribuinte no Ministério da Fazenda; III – se pessoa natural: a) nacionalidade; b) estado civil; c) números dos documentos de identidade e dos respectivos órgãos expedidores; d) filiação; e d) endereço residencial ou domiciliar. IV – se pessoa jurídica ou assemelhada, endereço da sede; e V – a relação dos feitos distribuídos em tramitação contendo os números, suas classes e os juízos da tramitação originária” (BRASIL, 2010).

Neste particular, mostra-se incompreensível a vinculação à grande quantidade de dados pessoais, sendo que o parágrafo segundo do mesmo art. 7º esclarece que estes se tratam para expedição da certidão: “§ 2º. A ausência de alguns dos dados não impedirá a expedição da certidão negativa se não houver dúvida quanto à identificação física da pessoa” (BRASIL, 2010).

Ademais, não será incluído na relação dos feitos distribuídos o processo em que houver o gozo do benefício do *sursis* ou quando a pena já tiver sido extinta ou cumprida, salvo para instruir processo pela prática de nova infração penal ou outros casos expressos em lei.

A resolução determina que não será expedida certidão quando houver registro de processo referente a homônimo e a individualização dos respectivos processos não puder ser realizada por conta de alguma limitação de dados pelo Poder Judiciário.

A certidão judicial negativa é expedida eletronicamente por meio dos portais dos tribunais na internet, já a certidão judicial positiva pode ser expedida eletronicamente àqueles previamente cadastrados no sistema processual, conforme previsto no art. 12.

A resolução previu que os órgãos jurisdicionais de que tratam os incisos de I-A a VII, do art. 92, da CF, devem observar os seus termos, assim como já prevê que qualquer pessoa eventualmente prejudicada pela disponibilização de informação na rede mundial de computadores, em desconformidade com a referida resolução, poderá solicitar a retificação ao órgão jurisdicional responsável.

A resolução estabeleceu, também, as diretrizes sobre a divulgação de dados processuais eletrônicos na internet e sobre a expedição de certidões judiciais, assim como deu outras providências.

Partindo das diretrizes traçadas pela referida resolução, a Resolução de n. 139, do Conselho Superior da Justiça do Trabalho (CSJT), que complementa as Resoluções CNJ números 121 de 2010 e 143 de 2011, no âmbito do Judiciário Trabalhista, dispõe sobre quais medidas devem ser adotadas pelos tribunais regionais do trabalho para impedir ou criar obstáculos para a realização de pesquisa de nome de empregados com o intuito de elaboração das chamadas “listas sujas”, contendo informações sobre reclamantes, o que também interessa ao objeto deste estudo.

A Resolução de número 139, do CSJT, tem por finalidade atenuar os riscos pela utilização indevida de dados de reclamantes diante das dificuldades existentes de impedir a coleta e tratamento de dados do Diário Eletrônico da Justiça do Trabalho por meio de sistemas de buscas na rede mundial de computadores.

Tal resolução prevê, em seu artigo primeiro, que os Tribunais Regionais deverão adotar medidas para impedir o acesso automatizado aos dados disponibilizados que estão presentes nos autos das reclamações trabalhistas, para evitar a elaboração das “listas sujas”, devendo ser respeitado o princípio da publicidade dos atos processuais e as previsões legais.

Dentre estas ações, prevê o parágrafo primeiro do referido artigo que os Tribunais Regionais deverão adotar ações que criem obstáculos ao rastreamento e às indexações “indesejadas” pelos sites de buscas, listando as providências por meio de um anexo, que poderão ser atualizadas periodicamente conforme previsto no artigo 2º.

Estas resoluções estabelecem um tratamento uniforme de divulgação dos atos processuais judiciais que deverá ser seguido pelos tribunais, no intuito de consolidar um padrão nacional de definição de níveis de publicidade das informações judiciais, para o exercício da transparência.

### 1.3 OS PROCESSOS EM SEGREDO DE JUSTIÇA

Como já apontado, o sistema jurídico prevê hipóteses de relativização ao princípio da publicidade dos atos processuais. A sistemática do processo civil, partindo das balizas traçadas pela Constituição Federal, prevê a possibilidade de decretação do segredo de justiça<sup>8</sup>, relativizando o princípio da publicidade.

O Código de Processo Civil disciplina hipóteses de segredo de justiça no seu artigo 189<sup>9</sup>, nos seguintes termos:

Art. 189. Os atos processuais são públicos, todavia tramitam em segredo de justiça os processos:

I - em que o exija o interesse público ou social;

II - que versem sobre casamento, separação de corpos, divórcio, separação, união estável, filiação, alimentos e guarda de crianças e adolescentes;

III - em que constem dados protegidos pelo direito constitucional à intimidade;

IV - que versem sobre arbitragem, inclusive sobre cumprimento de carta arbitral, desde que a confidencialidade estipulada na arbitragem seja comprovada perante o juízo.

§ 1º O direito de consultar os autos de processo que tramite em segredo de justiça e de pedir certidões de seus atos é restrito às partes e aos seus procuradores.

---

<sup>8</sup> No relatório da análise realizada sobre o tratamento de dados pessoais na consulta de jurisprudência, pontuou o CNJ (2021, p. 18) que: “A propósito da utilização do segredo de justiça como medida de proteção de dados pessoais, deve-se ressaltar a importância da colaboração das partes e dos auxiliares da justiça, desde a fase inicial de tramitação dos processos, para garantir a efetividade do instituto. 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)”.

<sup>9</sup> Neste particular, sobre a questão do sigilo, esclarece Cardoso (2021, p. 3) que: “O § 1º do art. 189 do CPC ressalva que o sigilo é extraprocessual, ou seja, apenas as partes e seus advogados têm acesso aos atos processuais, além de, excepcionalmente, terceiro juridicamente interessado (sobre parte do ato). Por isso, há uma pseudoanonimização dos dados (isto é, uma anonimização reversível), considerando que no julgamento desses processos, na movimentação processual e nos atos processuais, as partes são identificadas apenas por suas iniciais, a fim de impedir a identificação dos titulares dos dados e, ao mesmo tempo, respeitar o princípio da publicidade processual.”



§ 2º O terceiro que demonstrar interesse jurídico pode requerer ao juiz certidão do dispositivo da sentença, bem como de inventário e de partilha resultantes de divórcio ou separação (BRASIL, 2015).

No mesmo sentido, o art. 770, da Consolidação das Leis do Trabalho (CLT), prevê que “os atos processuais serão públicos salvo quando o contrário determinar o interesse social, e realizar-se-ão nos dias úteis das 6 (seis) às 20 (vinte) horas” (BRASIL, 1943).

Em sentido semelhante, prevê o art. 201, sexto parágrafo, do Código de Processo Penal que:

O juiz tomará as providências necessárias à preservação da intimidade, vida privada, honra e imagem do ofendido, podendo, inclusive, determinar o segredo de justiça em relação aos dados, depoimentos e outras informações constantes dos autos a seu respeito para evitar sua exposição aos meios de comunicação (BRASIL, 1941).

A publicidade especial, decorrente do segredo de justiça, justifica-se em caso de interesse social ou na defesa de direitos da personalidade, tendo os referidos artigos elencados hipóteses.

Analisando o processo civil, Marinoni, Arenhart e Mitidiero (2016, p. 308) pontuam:

Os atos processuais são públicos, só podendo ser restringida a publicidade do processo quando o exigir o interesse social ou a defesa da intimidade das partes. Nessa linha, os incisos do art. 189, CPC, refletem exatamente essa diretriz constitucional. A regra é a publicidade geral, sendo acessível a todos os atos processuais, aí incluído o direito de consultar os autos, de assistir audiências e de pedir certidões. Quando há segredo de justiça há publicidade especial (art. 189, parágrafo 1º do CPC).

O referido sigilo é em relação a terceiros, pois, em princípio, inexistente sigilo endoprocessual, que restrinja o acesso a informações pelas partes.

Neste sentido, Cardoso (2021, p. 2) sinaliza que:

A publicidade dos atos processuais é a regra no Brasil. Excepcionalmente a Constituição restringe a publicidade externa ou extraprocessual, ou seja, admite o sigilo extraprocessual, por uma razão: para preservar o direito à intimidade do interessado, quando isto não prejudicar o interesse público à informação. Logo, não existe processo sigiloso para as partes, segundo a Constituição. O sigilo só pode ser adotado em relação a terceiros. Em outras palavras, é permitido o sigilo extraprocessual (externo), mas não o endoprocessual (interno): as partes têm o direito fundamental de acesso e conhecimento a todos os atos do processo, sem exceção.

No entanto, embora não seja comum, alguns juízes optam por manter em sigilo documentos juntados pelas partes, inclusive em relação à parte contrária.

A título de exemplo, apresenta-se a hipótese de juntada de documento relativo à comprovação do seu estado de carência ou não econômica, que justifique a concessão do benefício da assistência judiciária econômica.<sup>10</sup>

Nesta hipótese, quando o juiz constata – por meio do documento protocolado em sigilo pelo interessado (via de regra, a declaração de imposto de renda) – que não há carência econômica, o juiz opta por manter o documento inacessível sob o fundamento de sigilo fiscal.

Há, ainda, a hipótese prevista no art. 773, do CPC, no sentido de que “O juiz poderá, de ofício ou a requerimento, determinar as medidas necessárias ao cumprimento da ordem de entrega de documentos e dados”, sendo que o parágrafo único do referido artigo ainda disciplina que “quando, em decorrência do disposto neste artigo, o juízo receber dados sigilosos para os fins da execução, o juiz adotará as medidas necessárias para assegurar a confidencialidade” (BRASIL, 2015).

O direito de consultar os autos e de requerer certidões de processos em que haja a decretação do segredo de justiça é limitada às partes e aos seus procuradores. Nos termos do parágrafo segundo do art. 189, do CPC, o terceiro, que eventualmente demonstre interesse

---

<sup>10</sup> Em sentido contrário e demonstrando o entendimento majoritário, já decidiu o Tribunal de Justiça do Distrito Federal e Territórios que: “DIREITO PROCESSUAL CIVIL. AGRAVO DE INSTRUMENTO. AGRAVO INTERNO. AÇÃO DE CONHECIMENTO. SIGILO DE DOCUMENTOS FISCAIS E BANCÁRIOS. NEGATIVA DE ACESSO À PARTE ADVERSA. IMPOSSIBILIDADE. VIOLAÇÃO AOS PRINCÍPIOS DO CONTRADITÓRIO E DA AMPLA DEFESA. GARANTIA DE ACESSO AOPROCESSO PELAS PARTES. APARENTE CONFLITO ENTRE O DIREITO À INTIMIDADE E O DIREITO AO CONTRADITÓRIO E AMPLA DEFESA. PONDERAÇÃO DE PRINCÍPIOS. DECISÃO MANTIDA. AGRAVO INTERNO PREJUDICADO. 1. A decretação do sigilo de documentos é medida excepcional, que afasta a regra da publicidade dos atos processuais e visa impedir que terceiros tenham acesso às informações sensíveis existentes nos autos, mas não se presta, jamais, a impedir a parte contrária de ter conhecimento do conteúdo sobre os quais recaem o sigilo. 2. Não é possível impedir a parte ré de ter acesso aos documentos que instruem os autos, ainda que sigilosos, sobretudo quando serviram para formar o convencimento do juiz sobre matéria levada à apreciação, sob pena de violação frontal aos princípios da ampla defesa e do contraditório. 3. Tratando-se de aparente conflito entre o direito à intimidade do autor e o direito do réu ao contraditório e à ampla defesa, a decretação de sigilo dos documentos que ostentam conteúdo sensível e a permissão de acesso apenas às partes é a solução que melhor atende aos fins da justiça, por quanto não afasta completamente os direitos questionados nem despreza integralmente o sentido de proteção previsto em ambos. 4. Agravo de Instrumento conhecido e não provido. Agravo interno prejudicado. Unânime (BRASIL. TJ-DFT. 3ª Turma. Processo n. 0707858-40.2021.8.07.0000. Relatora Desa. Fátima Rafael. Agravante Josyellen Crysthyna Martins de Araujo. Agravados: Bruno Alvarenga Silva Loredó, Instituto da Face e Otorrinolaringologia Ltda e Rede D’OR São Luiz S.A. Julgado em 09/06/2021. Publicado no DJE 23.06.2021. Disponível em: <https://pesquisajuris.tjdft.jus.br/IndexadorAcordaos-web/sistj>. Acesso em: 29 mar. 2024)”.

fundamentado, pode requerer uma certidão de dispositivo de sentença, assim como também de inventário e da partilha que resulte de ação de divórcio ou separação.

Ademais, prevê o parágrafo único do artigo 11, do CPC: “Nos casos de segredo de justiça, pode ser autorizada a presença somente das partes, de seus advogados, de defensores públicos ou do Ministério Público” (BRASIL, 2015).

A princípio, pode-se questionar se o referido rol, previsto no art. 189 do CPC, seria taxativo ou não. Ocorre que, com base na leitura do próprio dispositivo contido no artigo, pode-se perceber que não há taxatividade, até mesmo porque este traz cláusulas em aberto.

Sobre a ausência de taxatividade do rol previsto no art. 189, do CPC, Gomes Junior e Ferreira (2015, p. 135) apontam:

Não se verifica que a regra do art. 189 do NCPD seja taxativa. O fato é que foram utilizados tantos conceitos vagos pelo legislador que há ampla liberdade do Juízo, dentro da prudência e das regras constitucionais, que possa haver o deferimento de pedido de tramitação de um determinado caso em segredo de justiça. Um exemplo pode deixar tal ponto evidenciado, como a existência de dados sensíveis no feito ou mesmo a extensão do patrimônio em discussão. Entende-se que não há uma clara opção pelo regime da *taxatividade*, especialmente quando considerada a riqueza das relações jurídicas e as suas particularidades.

Diante das cláusulas abertas, para que seja decretado o segredo de justiça, é necessário um exercício de interpretação do órgão judicial que poderá atender ou não a expectativa do jurisdicionado.<sup>11</sup>

---

<sup>11</sup> A título exemplificativo, segue julgado do Superior Tribunal de Justiça sobre o tema, em que não foi acolhido o pedido de decretação de segredo de justiça, muito embora tenha sido sustentada a existência de “*documentos comerciais sensíveis*” e de apólices que contêm “*dados de valor estratégico*”: “AGRAVO EM RECURSO ESPECIAL Nº 1.301.454 - ES (2018/0128396-4) RELATOR: MINISTRO LÁZARO GUIMARÃES (DESEMBARGADOR CONVOCADO DO TRF 5ª REGIÃO) AGRAVANTE: SAMARCO MINERACAO S.A ADVOGADOS: ELIANE CRISTINA CARVALHO TEIXEIRA - SP163004 ALESSANDRA PATRÍCIA DE SOUZA ALBUQUERQUE - ES013181 THIAGO BRAGANÇA - ES014863 PAULO EDUARDO LEITE MARINO - SP276599 TICIANA FONSECA FAVIERO - RJ178971 AGRAVADO: MINISTÉRIO PÚBLICO DO ESTADO DO ESPÍRITO SANTO. DECISÃO Trata-se de agravo em recurso especial interposto por SAMARCO MINERACAO S.A, doravante SAMARCO, contra decisão exarada pela il. Vice-Presidência do eg. Tribunal de Justiça do Estado do Espírito Santo (TJ-ES), que inadmitiu o recurso especial. Cuida-se de agravo de instrumento manejado por SAMARCO nos autos da ação cautelar de exibição de documentos movida por MINISTÉRIO PÚBLICO DO ESTADO DO ESPÍRITO SANTO. O eg. TJ-ES deu parcial provimento ao recurso, nos termos do v. acórdão, assim ementado (fls. 506/507): "AGRAVO DE INSTRUMENTO. AÇÃO DE EXIBIÇÃO DE DOCUMENTOS. REQUERIMENTO DE EXIBIÇÃO DE SEGUROS E RESSEGUROS. DESNECESSIDADE. MULTA COMINATÓRIA. IMPOSSIBILIDADE. RECURSO CONHECIDO E PARCIALMENTE PROVIDO. 1. (...) Decido. Cumpre salientar que o presente recurso será examinado à luz do Enunciado 3 do Plenário do STJ:"Aos recursos interpostos com fundamento no CPC/2015 (relativos a decisões

Caso não haja a decretação do segredo de justiça, a publicidade geral dos dados processuais prevalece, por ser a regra geral em nome da transparência.

Neste sentido, entendem Gomes Junior e Ferreira (2015, p. 134):

Desta forma, a viga mestre é a de que os procedimentos administrativos e processos judiciais sejam públicos, sendo a exceção que a tramitação ocorra com segredo de justiça. O objetivo é claro: a-) tornar viável que os atos praticados sejam fiscalizados; b-) uma garantia em favor do julgador perante a comunidade de que o mesmo agiu com imparcialidade. Deve ainda ser anotado que tal garantia tem a natureza de direito fundamental, ou seja, o de assegurar a existência de um julgamento de imparcialidade. Adequado ponderar que o Supremo Tribunal Federal tem sido *extremamente rigoroso* na defesa da total transparência dos atos processuais, considerando a relevância que é para a credibilidade do Poder Judiciário e de suas decisões com a mais ampla publicidade.

Vale frisar que, dentre as hipóteses previstas no art. 189, o inciso III merece uma atenção especial neste estudo, pois prevê a possibilidade de decretar o segredo de justiça em processos em que existam dados protegidos pelo direito constitucional à intimidade.

É com base no referido inciso e na LGPD que se pretende defender a possibilidade de decretação de segredo de justiça nos casos em que existam dados pessoais sensíveis nos atos processuais, o que se verá em tópico subsequente.

---

publicadas a partir de 18 de março de 2016) serão exigidos os requisitos de admissibilidade recursal na forma do novo CPC. "No apelo nobre que pretende trânsito, sustenta o recorrente ofensa do art. 155 do CPC/73 (atual art. 189 do CPC/2015) e do art. 206 da Lei n.º 9.279/96, ao argumento de que a presente demandaria deveria tramitar sob segredo de justiça. Afirma-se que o rol previsto no Código de Processo Civil é meramente exemplificativo, bem como ressalta que a Lei de Propriedade Intelectual prevê a possibilidade de sigilo quanto aos documentos comerciais sensíveis. Alega, por fim, que as apólices de seguro, cuja exibição foi determinada na origem, contêm dados de valor estratégico, motivo pelo qual demandam a necessária confidencialidade. O recurso, contudo, não merece prosperar. Isso porque o eg. TJ-ES, mediante análise soberana das provas carreadas aos autos, negou o segredo de justiça sob os seguintes fundamentos: (i) a presente demanda não se enquadra em qualquer hipótese prevista no art. 155 do CPC/73; e (ii) a apresentação apenas das apólices de responsabilidade civil não é apta a causar danos ao recorrente. À título elucidativo, colaciona-se o seguinte excerto do v. acórdão estadual (fl. 516): "Desse modo, analisando as hipóteses legais de previsão de decretação do sigilo na tramitação, a exemplo do art. 155, do CPC de 1973, observo que os autos em comento não versam sobre quaisquer hipóteses ensejadoras de tal trâmite. Além disso, considerando que restou determinada a apresentação apenas das apólices de responsabilidade civil, tenho que a retirada do sigilo de tramitação deste processo não tem o condão de causar danos ao agravante, razão pela qual retiro a decretação de processamento em segredo de justiça". Nesse cenário, para se alterar o entendimento ora transcrito, quanto ao descabimento do segredo de justiça, seria necessária a revisão de matéria fático-probatória, o que é inadmissível em sede de recurso especial, nos termos da Súmula 7/STJ. Assim, forçoso reconhecer que o presente apelo não merece prosperar. Diante do exposto, nos termos do art. 253, parágrafo único, II, b, do RISTJ, conheço do agravo para negar provimento ao recurso especial. Publique-se. Brasília (DF), 25 de junho de 2018. MINISTRO LÁZARO GUIMARÃES (DESEMBARGADOR CONVOCADO DO TRF 5ª REGIÃO) Relator". (BRASIL. STJ - AREsp: 1301454 ES 2018/0128396-4, Relator: Ministro LÁZARO GUIMARÃES (DESEMBARGADOR CONVOCADO DO TRF 5ª REGIÃO), Data de Publicação: DJ 27/06/2018).

Sobre o referido dispositivo, Zanetti (2021) pondera que:

Na busca de dar concretude ao mandamento constitucional estabelecido pelo art. 5º, LV, o Código de Processo Civil apresenta os limites objetivos para a caracterização da necessidade de dar sigilo aos atos processuais, como se verifica nas hipóteses previstas nos incisos do art. 189, que dependem da existência de: (I) interesse público ou social pelo segredo; (II) processos que versem sobre casamento, separação de corpos, divórcio, separação, união estável, filiação, alimentos e guarda de crianças e adolescentes; (III) dados protegidos pelo direito constitucional à intimidade; e (IV) processos que versem sobre arbitragem, inclusive sobre cumprimento de carta arbitral, desde que a confidencialidade estipulada na arbitragem seja comprovada perante o juízo.

Das quatro hipóteses acima, aquela que melhor reflete o argumento daqueles que fundamentam na LGPD a necessidade do sigilo processual, notoriamente, é a do inciso III, referente a dados que merecem proteção para preservação da intimidade de seu titular.

No entanto, é fundamental observar que a proteção de dados pessoais, como dito, é direito autônomo e, conseqüentemente, diverso da intimidade. Aqui, a noção de intimidade não deve ser alargada para compreender todo e qualquer dado pessoal, ou seja, toda e qualquer "informação relacionada a pessoa natural identificada ou identificável", conforme definição do art. 5º, I, da LGPD.

O simples fato de o dado pessoal constar em um processo judicial não retira deste a condição de bem juridicamente protegido e que, nesta linha, merece atenção e proteção.<sup>12</sup> Ademais, é evidente que a existência de dados pessoais em um processo judicial não justificaria, *a priori*, a decretação de segredo de justiça.<sup>13</sup> Caso contrário, todos os processos judiciais clamariam pela decretação de segredo de justiça.

<sup>12</sup> Neste sentido, o Tribunal de Justiça do Distrito Federal e Territórios já decidiu: “AGRAVO DE INSTRUMENTO. EXECUÇÃO DE TÍTULO EXTRAJUDICIAL. PETIÇÃO. ANOTAÇÃO DE SIGILO. PRESERVAÇÃO DA INTIMIDADE E PRIVACIDADE. NECESSIDADE. DECISÃO REFORMADA. 1. Como o segredo de justiça é exceção a um princípio de status constitucional, as normas que o disciplinam deverão ser interpretadas restritivamente, sendo inegável, todavia, que a declaração de imposto de renda é protegida pelo sigilo fiscal. 2. Transcritos, em petição juntada aos autos, longos trechos das declarações de imposto de renda dos executados-agravantes, expondo informações de terceiros e relações de família, imprescindível a atribuição de sigilo à peça. 3. Agravo conhecido e provido”.(BRASIL. TJ-DFT. 7ª Turma Cível. Processo n. 0710842-94.2021.8.07.0000. Relator Des. Fabio Eduardo Marques. Agravante Jose Celso Valadares Gontijo e Ana Maria Baeta Valadares Gontijo. Agravados: BRB Banco de Brasília S.A. Julgado em 25/08/2021. Publicado no DJE 18.08.2021. Disponível em: <https://pesquisajuris.tjdft.jus.br/IndexadorAcordaos-web/sistj>. Acesso em: 29 mar. 2024)

<sup>13</sup>A Resolução 185 de 2013 do CNJ, que instituiu o Sistema Processo Judicial Eletrônico (PJE) como sistema de processamento de informações e prática de atos processuais prevê que: “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 § 4º Nos casos em que o rito processual autorize a apresentação de resposta em audiência, facultar-se a sua juntada antecipada aos autos eletrônicos, juntamente com os documentos, hipótese em que permanecerão ocultos para a parte contrária, a critério do advogado peticionante, até a audiência”.

Numa petição inicial, como já exemplificado, existem informações sobre a pessoa que compreendem, basicamente, a qualificação e eventuais particularidades pessoais, além dos fatos que envolvem a causa de pedir. Cumpre esclarecer que, para este estudo, a causa de pedir é entendida como o conjunto de fatos e a relação jurídica apontados como fundamentos da ação.

Neste sentido, entende Didier Júnior (2022, p. 708) que a “causa de pedir é o fato ou conjunto de fatos jurídicos (fato(s) da vida juridicizado(s) pela incidência da hipótese normativa) e a relação jurídica, efeito daquele fato jurídico, trazidos pelo demandante como fundamento do seu pedido”.

As informações relacionadas à mera qualificação, que não justificam a decretação do segredo de justiça, por não ser possível um “alargamento” do conceito de intimidade, devem ser sempre objeto de um sigilo seletivo, com restrição de acesso. Afinal, os referidos dados não podem permanecer em situação de vulnerabilidade e o interesse público não justificaria sua exibição indiscriminada, especialmente diante da nova realidade trazida com os avanços tecnológicos e com a LGPD.

Atualmente, não se pode desconsiderar que o novo instrumental tecnológico pode causar violações à intimidade, à privacidade, à autodeterminação informativa e à proteção de dados, possibilidades que se tornaram riscos em potencial.

Sobre o processo digital e o segredo de justiça, Doneda e Machado (2021, p. 334) afirmam que:

No âmbito de tratamento de dados pelo Estado, tal situação pode ser mais bem compreendida por meio de um paralelo com a informatização do processo eletrônico e o cumprimento do princípio da eficiência. É inegável que entre as vantagens do processo eletrônico está a ampliação da eficiência do poder judiciário. Todavia, a implementação da solução leva em consideração uma série de questões relacionadas à segurança e à confidencialidade de alguns atos. Assim, a regulação do processo

---

Já a Resolução 185 de 2017, do CSJT, que dispõe sobre a padronização do uso, governança, infraestrutura e gestão do Processo Judicial Eletrônico instalado na Justiça do Trabalho, alterada pela Resolução de n. 241 de 2019 do CSJT, prevê nos parágrafos 2º, 3º, 4º e 5º do seu artigo 22, que tratam do segredo de justiça que: “§ 2º O autor poderá atribuir segredo de justiça ao processo no momento da propositura da ação, cabendo ao magistrado, após a distribuição, decidir sobre a manutenção ou exclusão dessa situação, nos termos do art. 189 do CPC e art. 770, caput, da CLT. § 3º Com exceção da petição inicial, as partes poderão atribuir sigilo às petições e documentos, nos termos do parágrafo único do art. 773 do CPC. § 4º Com exceção da defesa, da reconvenção e dos documentos que as acompanham, o magistrado poderá determinar a exclusão de petições e documentos indevidamente protocolados sob sigilo, observado o art. 15 desta Resolução. § 5º O réu poderá atribuir sigilo à contestação e à reconvenção, bem como aos documentos que as acompanham, devendo o magistrado retirar o sigilo caso frustrada a tentativa conciliatória”.

eletrônico, além de ter sido realizada por lei e não por decreto, contém previsões específicas acerca da garantia da integridade dos dados e da indicação da preservação do segredo de justiça. Este exemplo demonstra uma situação em que se atende ao princípio da eficiência sem afastar a necessária proteção de dados.

Quanto às eventuais particularidades pessoais, o que incluiria os dados sensíveis acerca da pessoa, especialmente se esta condição tiver relevância à causa de pedir (a exemplo de uma doença ou de uma crença religiosa), esta tese busca defender que não seria apenas o caso de um sigilo seletivo, mas sim da decretação do segredo de justiça por tocar a intimidade.

Diante disto, faz-se necessária uma ponderação de interesses e a definição de parâmetros para definir os níveis de publicidade e a limitação<sup>14</sup> de acesso a informações constantes nos atos processuais, salvaguardando os dados pessoais, para que estes dados efetivamente gozem de proteção.

Tal providência faz-se necessária, atualmente, à medida que, cada vez mais, os aludidos dados estão passíveis de mercantilização, diante do desenvolvimento e aprimoramento de técnicas de cruzamento de informações, a partir do uso de refinados meios tecnológicos.

---

<sup>14</sup> Doneda e Machado (2021, p. 346) pontuam que: “Já se disse que o fato de um órgão da administração pública manter um dado sob seu poder não significa que possa utilizá-lo para qualquer finalidade. A limitação da finalidade implica considerar que nem internamente, dentro do próprio órgão, os dados poderiam ser usados para qualquer finalidade. Uma consequência natural disso é a consideração de que os órgãos da administração não podem livremente compartilhar dados entre si pelo simples fato de pertencerem à administração”.

## 2. O DIREITO FUNDAMENTAL À PRIVACIDADE, À INTIMIDADE, À AUTODETERMINAÇÃO INFORMATIVA E À PROTEÇÃO DE DADOS

### 2.1 EXTENSÃO DA PRIVACIDADE, DA INTIMIDADE E DA AUTODETERMINAÇÃO INFORMATIVA

O artigo 5º da Constituição Federal, em seu inciso X, prevê que a intimidade, a vida privada, a honra e a imagem das pessoas são invioláveis, anunciando ainda o direito ao ressarcimento no caso de danos materiais e morais resultantes da violação.

Nesta linha, a privacidade e a intimidade são essenciais para o exercício da personalidade, sendo que a privacidade está relacionada à vida privada, aos aspectos do papel do indivíduo na sociedade, o que envolve sua profissão, posicionamentos ideológicos e políticos, dentre outros, que evidenciam sua liberdade na forma de conduzir a vida.

Já a intimidade envolve as relações mais íntimas, pois está relacionada àquilo que o indivíduo guarda para si, que envolve as escolhas pessoais, a exemplo da orientação sexual ou o fato de ser portador de alguma enfermidade, sendo que o indivíduo é livre para decidir com quem vai compartilhar estas informações.

Alessandro Hirata (2017), em relação à origem do termo privacidade e à distinção ao direito à intimidade, sustenta que:

A origem do termo privacidade no campo jurídico remete ao “*right to privacy*”. A privacidade (*privacy*) pode ser definida como o direito de estar só ou, talvez mais preciso, o direito de ser deixado só (“*right to be let alone*”). Assim, entende-se que a privacidade pode sofrer ataques, podendo gerar desgastes e dores muito maiores que uma injúria corporal.

Ainda que bastante vaga, essa primeira concepção de privacidade deve ser interpretada como sendo o “direito de ser deixado só”, que remete à não interferência pelo Estado na vida do indivíduo. Todavia, deve-se entender a privacidade não apenas como a não interferência do Estado na vida do indivíduo, mas também como o poder de se reivindicar ao Estado a tutela dessa privacidade, protegendo o indivíduo de terceiros.

Na sociedade contemporânea, porém, a noção de privacidade extravasa os conceitos de isolamento ou tranquilidade. O “*right to be let alone*” revela-se insuficiente em uma sociedade em que os meios de violação da privacidade caminham paralelamente aos diversos e importantes avanços tecnológicos.

Cabe lembrar, que alguns autores distinguem o direito à intimidade do direito à vida privada. A. De Cupis, por exemplo, entende que a esfera íntima da pessoa se divide em direito à *riservatezza* e o direito à *segretezza*. O direito à intimidade pode ser



conceituado como aquele que visa a resguardar as pessoas dos sentidos alheios, principalmente da vista e dos ouvidos de outrem. Ou seja, é o direito da pessoa de excluir do conhecimento de terceiros tudo aquilo que a ela se relaciona. O direito à intimidade é, ainda, o poder correspondente ao dever de todas as outras pessoas de não se imiscuir na intimidade alheia, opondo-se a eventuais descumprimentos desse dever, realizados por meio de investigação e/ou divulgação de informações sobre a vida alheia.

Como direitos da personalidade, estes são objeto de uma tutela diferenciada no ordenamento jurídico nacional, sendo que o Código Civil, em seus artigos 11 e 21, prevê que “com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária” e que “a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma” (BRASIL, 2002).

Mendes e Fonseca (2021, p. 76-77) destacam que:

Nas palavras de Stefano Rodotà, ocorreu um verdadeiro “processo inexorável de reinvenção da privacidade” na medida em que novas tecnologias da informação e da comunicação (TICs) penetraram a vida social e as dinâmicas político-econômicas (público e privadas), alterando sensivelmente os fluxos de informação”. Nesse contexto, muitas das discussões regulatórias começaram a se referir ao direito à proteção de dados pessoais, concebido para além de uma mera decorrência da privacidade: um direito fundamental autônomo cujo âmbito de proteção está vinculado à tutela da dignidade e da personalidade dos cidadãos no seio da sociedade da informação.

A privacidade e a intimidade, pelas características da sociedade atual, têm adotado também uma nova abordagem relacionada ao controle sobre a disponibilização de informações pessoais, reconhecida como autodeterminação informativa

Neste sentido, pontua Alimonti (2020, p. 180) que:

A noção de controle da pessoa sobre o fluxo de seus próprios dados se fortalece em face de uma concepção mais tradicional da privacidade. Na disciplina herdeira de proteção de dados pessoais, mesmo informações conhecidas ou de acesso público devem ser objeto de proteção, e protegê-las não significa necessariamente ocultá-las, guardá-las em segredo. Trata-se, antes, de estabelecer mecanismos de regulação do fluxo de informação e instituir procedimentos de controle. Como visto, mecanismos de regulação e procedimentos ligados ao princípio de proteção de dados que se desdobram em direitos subjetivos do titular, como direito de acesso e retificação, além do próprio consentimento informado enquanto mecanismo central a autorizar o tratamento de dados pessoais. A preocupação em tutelar fluxo de dados pessoais deriva justamente da relação desses dados com pessoas, identificadas ou potencialmente identificáveis, e do fato de seu tratamento ser capaz de gerar efeitos diretos na esfera de direitos de seus titulares.

Da autodeterminação informativa decorre o entendimento de que, em regra, somente o próprio titular pode decidir sobre a disponibilização, processamento e transmissão dos seus dados. No entanto, em situações excepcionais e regulamentadas por lei, este direito pode vir a ser mitigado em face do interesse público.

Sobre a evolução das ideias relacionadas à privacidade, Facchini Neto e Demoliner (2018, p. 25-26) defendem que:

[...] as ideias sobre privacidade evoluíram no sentido de que se passou do direito a ser deixado só ao direito de ter sob controle as informações que nos dizem respeito; da privacidade ao direito à autodeterminação informativa; da privacidade à não-discriminação; do sigilo ao controle.

[...]

Entre nós, Doneda refere que nossos dados, devidamente sistematizados e aglutinados, significam nossa representação virtual. Quem tem acesso a eles pode decidir sobre conceder ou não um crédito, celebrar ou não um plano de saúde, conceder ou não uma vaga de emprego, e, se for um governo, autorizar ou não a entrada de alguém em seu país. Não por acaso vem se chamando a essa nossa representação virtual de “corpo eletrônico”, “avatar eletrônico”, “data shadow”. Enfim, chega-se quase à conclusão de que “somos o que o google diz que somos”: nossa biografia passa a ser definida pelo famoso algoritmo daquela multinacional.

Neste novo ambiente<sup>15</sup>, em que há uma verdadeira vigilância digital com fluxo constante de dados pessoais, a forma em que o tratamento de dados é realizado sofreu profundas alterações, como destaca Bezerra (2017, p. 1):

Para tanto, vale-se do contraste entre as formas de mediação da informação estabelecidas no século XX (e vigentes até o início do século XXI) e as novas formas de produção, circulação, mediação e acesso a informação. O principal ponto a ser destacado é a mudança de um perfil de mediação centrado na figura de editores e produtores para uma mediação a princípio lida como “tecnológica” - posto que encarnada por fórmulas matemáticas de algoritmos - mas que é concebida por engenheiros de grandes empresas como Google e Facebook, alimentada pelas informações dos próprios usuários das plataformas e utilizada tanto por empresas para finalidades econômicas quanto por governos em suas agendas políticas. Conclui-se que as mudanças na estrutura sociotécnica do “regime de informação” vigente (conforme autores como Bernd Frohmann e González de Gómez), embora permitam avanços nas mais diversas áreas (educação, saúde, segurança pública, consumo, mobilidade urbana e outros), podem trazer efeitos deletérios para a cultura e para a

---

<sup>15</sup>Esclarece, ainda, Bezerra (2017, p. 2): “A estrutura de vigilância do comportamento dos indivíduos que navegam pelas redes digitais é muitas vezes ignorada pelos usuários, ou seja, difere-se do panopticon tanto por seu aspecto distribuído quanto pela sua ação muitas vezes invisível, distanciando-se da ideia de autodisciplina e aproximando-se da realidade que Deleuze (1992) associa ao que, atualizando a “sociedade disciplinar” de Foucault, chama de “sociedade de controle”. Quando não ignorada, essa vigilância é muitas vezes consentida pelos indivíduos, seja por questões de segurança pública (LYON, 2010; CARDOSO, 2014) ou pelas vantagens que promete na customização de ofertas de bens de consumo (ANDERSON, 2009). A privacidade, tão importante para o individualismo forjado ao longo do período moderno, torna-se refém dos usos das técnicas de vigilância digital, seja por empresas ou governos”.

criatividade humana, principalmente no que se refere à privacidade e ao acesso a um conjunto diversificado de artefatos culturais, científicos e informativos.

O Ministro Gilmar Mendes, no julgamento conjunto das Ações Diretas de Inconstitucionalidade (ADIN) referentes à Medida Provisória de número 954, de 2020, esclareceu pontos sobre a abordagem da privacidade e da autodeterminação informativa neste novo momento social:

Essa nova abordagem (*da privacidade*) também engloba uma proteção abrangente que desloca o eixo da proteção do conteúdo dos dados para as possibilidades e finalidades do seu processamento. Como bem destacado pela professora Laura Schertel Mendes, é decisivo para a concepção do direito à autodeterminação “*o princípio segundo o qual não mais existiriam dados insignificantes nas circunstâncias modernas do processamento automatizado dos dados*”, de modo que “*o risco do processamento de dados residiria mais na finalidade do processamento e nas possibilidades de processamento do que no tipo dos dados mesmos (ou no fato que quão sensíveis ou íntimos eles são)*” (MENDES, Laura Schertel. Autodeterminação informativa: a história de um conceito. *No Prelo*).

[...]

A afirmação de um direito fundamental à privacidade e à proteção de dados pessoais deriva, ao contrário, de uma compreensão integrada do texto constitucional lastreada (i) no direito fundamental à dignidade da pessoa humana, (ii) na concretização do compromisso permanente de renovação da força normativa da proteção constitucional à intimidade (art. 5º, inciso X, da CF/88) diante do espraiamento de novos riscos derivados do avanço tecnológico e ainda (iii) no reconhecimento da centralidade do *Habeas Data* enquanto instrumento de tutela material do direito à autodeterminação informativa”.

[...]

A rigor, entre nós, há mais de duas décadas, já se ensaia a evolução do conceito de privacidade a partir da edição de legislações setoriais que garantem a proteção de dados pessoais, tais como o Código de Defesa do Consumidor, a Lei do Cadastro Positivo, a Lei de Acesso à Informação, o Marco Civil da Internet – que inclusive assegura aos usuários da internet, entre outros direitos, a inviolabilidade e o sigilo do fluxo de comunicações e dos dados armazenados (art. 7º, II e III) – e, mais recentemente, a Lei Geral de Proteção de Dados (Lei 13.709/2018). Este último diploma assenta de maneira clara que “*a disciplina da proteção de dados pessoais tem como fundamentos o respeito à privacidade e a autodeterminação informativa* (art. 2º, incisos I e II). (BRASIL. Supremo Tribunal Federal. Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.390. Relator: Ministro Rosa Weber. Plenário. Disponível em: [www.stf.jus.br](http://www.stf.jus.br). Acesso em: 4 ago. 2021).

Neste mesmo julgamento conjunto das ADINs referentes à MP 954/2020, o voto da Ministra Relatora ressaltou o desafio enfrentado na atualidade pelo direito à privacidade:

14. Entendo que as condições em que se dá a manipulação de dados pessoais digitalizados, por agentes públicos ou privados, consiste em um dos maiores desafios contemporâneos do direito à privacidade.

A Constituição da República confere especial proteção à intimidade, à vida privada, à honra e à imagem das pessoas ao qualificá-las como invioláveis, enquanto direitos fundamentais da personalidade, assegurando indenização pelo dano material ou moral decorrente de sua violação (art. 5º, X). O assim chamado direito à privacidade (*righttoprivacy*) e os seus consectários direitos à intimidade, à honra e à imagem emanam do reconhecimento de que a personalidade individual merece ser protegida em todas as suas manifestações.

A fim de instrumentalizar tais direitos, a Constituição prevê, no art. 5º, XII, a inviolabilidade do “sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução penal”.

[...]

Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais”. (BRASIL. Supremo Tribunal Federal. Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.390. Relator: Ministro Rosa Weber. Plenário, p. 15-16. Disponível em: [www.stf.jus.br](http://www.stf.jus.br). Acesso em: 4 ago. 2021).

Ademais, a privacidade, a intimidade e a autodeterminação informativa têm relação próxima também com o direito fundamental ao “esquecimento”, que estaria fundado na dignidade da pessoa humana, assim como no desenvolvimento da personalidade. Este tema tem ganhado, a cada dia, maior destaque.

Em que pese não tenha previsão normativa expressa no ordenamento jurídico, este preenche os requisitos da fundamentalidade, a ser analisada no tópico subsequente, o que – no entender deste estudo – já justificaria o enquadramento como direito fundamental.

O direito ao esquecimento, neste sentido, visa garantir o direito de recomeçar sem marcas do passado que criam algum tipo de embaraço.

Neste sentido, pontua Sarlet (2020, p. 71) que:

Assim, em apertada síntese, é possível sustentar que o direito ao esquecimento, numa perspectiva da ordem constitucional brasileira, constitui um direito fundamental de natureza implícita, manifestação (e mesmo exigência) da dignidade da pessoa humana e do direito ao livre desenvolvimento da personalidade, guardando relação, ainda, com diversos direitos de personalidade consagrados – de modo explícito e implícito – pela CF, tais como os direitos à privacidade, intimidade, honra e imagem, mas também os direitos à autodeterminação informativa, ao nome e o direito à identidade pessoal, todos já reconhecidos pelo STF.

O direito ao esquecimento – que não é objeto deste estudo - implica não apenas direito ao cancelamento de dados, dentro da vertente deste trabalho, como também no direito à desindexação num ambiente de instrumentos de buscas na internet.

Diante desta mudança de paradigmas e do objeto do estudo, faz-se necessário um aprofundamento sobre o que seria o direito fundamental à proteção de dados.

## 2.2 O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS: O RECONHECIMENTO PELO SUPREMO TRIBUNAL FEDERAL

### 2.2.1 Noções gerais sobre a materialidade dos direitos fundamentais

Os direitos fundamentais, segundo Pulido (2014, p. 387), são “um tipo de direito subjetivo, cuja diferença reside em sua fundamentalidade”.

Existem direitos fundamentais não previstos na Constituição, mas que têm em seu conteúdo previsões diferenciadas, que são denominados por Robert Alexy (2008, p. 68) como sendo “normas de direito fundamental atribuídas”. Para ele, tais direitos decorreriam da evolução interpretativa de normas estabelecidas e representariam a criação de novos direitos fundamentais, que são desdobramento dos já estabelecidos, permitindo a evolução do sistema.

Sobre o tema explica Pulido (2014, p. 394) que:

Por outro lado, a jurisprudência permite atribuir caráter fundamental a determinadas normas legais e posições legais que não se encontram no campo semântico de uma disposição fundamental. Esse é o caso do assim chamado reconhecimento de direitos fundamentais não escritos por meio da jurisprudência constitucional. Não se trata aí de direitos fundamentais atribuídos (*zugeordnet*), mas de direitos fundamentais sem disposição fundamental. Algumas constituições preveem expressamente a validade de direitos fundamentais sem disposições de direitos fundamental, bem como a validade de direitos fundamentais não escritos. Um caso conhecido é a emenda nove da Constituição dos Estados Unidos da América, que diz: “a enumeração de determinados direitos na Constituição não deve ser feita de modo a negar ou limitar outros retidos pelo povo” (*The enumeration in the Consitution, of certain rights, shall not be construed to denyor disparage others retained by the people*). O art. 5º, LXXVIII, par. 2º da Constituição do Brasil e o art. 94 da Constituição da Colômbia possuem formulações semelhantes.

Neste particular, vale destacar o que dispõe o art. 5º, § 2º da Constituição Federal do Brasil: “Os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte” (BRASIL, 1988).

Ainda sobre as propriedades formais dos direitos fundamentais, pontua Pulido (2014, p. 395):

Como resultado da análise das propriedades formais, é possível afirmar que um direito fundamental manifesta fundamentalidade e com isso representa um direito fundamental quando preenche as seguintes condições: é estatuído por meio de uma disposição pertencente (1) ao capítulo dos direitos fundamentais da Constituição (2) ao texto da Constituição em geral ou (3) ao bloco constitucional; ou (4) a respectiva norma legal, bem como a posição legal, tenha sido reconhecida pela jurisprudência constitucional enquanto posição de direito fundamental, bem como norma de direito fundamental. (4) é por si só uma condição suficiente. É condição necessária que direitos subjetivos preencham uma das condições (1) a (4).

Após reconhecer que as propriedades formais não seriam suficientes para formular um conceito adequado da fundamentalidade dos direitos fundamentais, Pulido (2014, p. 400) sintetiza a questão das propriedades materiais nos seguintes termos:

As propriedades materiais da fundamentalidade dos direitos fundamentais devem ser compreendidas como condições suficientes que um direito subjetivo deve possuir para ser considerado direito fundamental. Consequentemente, um direito subjetivo deve ser reconhecido como direito fundamental quando proteger as habilidades morais do indivíduo liberal ou sua imputabilidade, bem como quando visar satisfazer as necessidades fundamentais do indivíduo. Soma-se a isso o fato de que um direito subjetivo se constitui como direito fundamental quando assegurar a igualdade em termos de sua habilidade liberal e imputabilidade dos indivíduos ou quando garantir a igualdade na distribuição dos bens que satisfazem as necessidades fundamentais. Um direito subjetivo precisa manifestar ao menos uma propriedade material para ser considerado um direito fundamental. Com isso, as propriedades materiais ganham prioridade em face das propriedades formais.

Neste sentido, Ingo Sarlet (2006, p. 95) pondera que

[...] direitos fundamentais em sentido material são aqueles que, apesar de se encontrarem fora do catálogo, por seu conteúdo e por sua importância podem ser equiparados aos direitos formalmente (e materialmente) fundamentais.

A materialidade estaria assentada em valores que são importantes para a sociedade, que, para este estudo, seriam a Dignidade da Pessoa Humana e o Estado Democrático de Direito, como base para os direitos fundamentais.

Como reconhecimento da sua importância, a Dignidade da Pessoa Humana foi incluída como fundamento da República Federativa do Brasil (BRASIL, 1988):

Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos:

- I – A soberania;
- II – A cidadania;
- III – A dignidade da pessoa humana;
- IV – Os valores sociais do trabalho e da livre iniciativa;
- V – O pluralismo político.

Tratando sobre a Dignidade da Pessoa Humana, esclarece Maria Celina Bodin de Moraes (2003, p. 77):

Para distinguir os seres humanos, diz-se que detêm uma substância única, uma qualidade própria apenas aos humanos: uma “dignidade” inerente à espécie humana. A raiz etimológica da palavra “dignidade” provém do latim *dignus* – “aquele que merece estima e honra, aquele que é importante”; diz-se que sua utilização correspondeu sempre a pessoas, mas foi referida, ao longo da Antiguidade, apenas à espécie humana como um todo, sem que tenha havido qualquer personificação.

Maria Celina Bodin de Moraes (2003, p. 85), aprofundando o tema, propõe a repartição do “substrato material da dignidade” em quatro postulados, a saber:

- i) o sujeito moral (ético) reconhece a existência dos outros como sujeitos iguais a ele,
- ii) merecedores do mesmo respeito à integridade psicofísica de que é titular;
- iii) é dotado de vontade livre, de autodeterminação;
- iv) é parte do grupo social, em relação ao qual tem a garantia de não vir a ser marginalizado. São corolários desta elaboração os princípios jurídicos da igualdade, da integridade física e moral – psicofísica -, da liberdade e da solidariedade.

A dignidade, portanto, representaria a concretização destes postulados, da qual decorreriam os direitos da personalidade.

Sobre a personalidade, ensina ainda Maria Celina Bodin de Moraes (2003, p. 121):

A personalidade é, portanto, não um “direito”, mas um valor, o valor fundamental do ordenamento, que está na base de uma série (aberta) de situações existenciais, nas quais se traduz a sua incessantemente mutável exigência de tutela. Por isso, não pode existir um número fechado (*numerusclausus*) de hipóteses tuteladas: tutelado é o valor da pessoa, sem limites, salvo aqueles postos no seu interesse e no interesse de outras pessoas humanas.

No intuito de garantir a Dignidade da Pessoa Humana, que assenta a materialidade dos direitos fundamentais, é imprescindível o estabelecimento do Estado Democrático de Direito - que é segundo valor eleito para embasar a fundamentação material dos direitos fundamentais - que também foi indicado pela Constituição Federal de 1988 como fundamento para a República Federativa do Brasil.

No Estado Democrático de Direito, a soberania popular é que legitima a atuação estatal, em um ambiente no qual se deve salvaguardar as liberdades individuais.

Barros, Branco e Pamplona Filho (2010, p. 83) destacam também que:

Por este motivo, defende-se que a fundamentalidade material decorre da realização da igualdade jurídica e social, logrando-se êxito, neste sentido, em alcançar um conteúdo não espiritual dos direitos fundamentais, a partir dos seus fundamentos de materialidade.

Logo, o processo de materialização dos direitos fundamentais, ao mesmo tempo em que corresponde ao pensamento de que existe uma especial importância no objeto tutelado por estas normas, corresponde também à atribuição de conteúdo referenciado com os guias axiológicos às normas positivadas.

Com isso, conduz-se a uma visão otimista da defesa dos direitos fundamentais no Brasil: o processo de derivação de direitos fundamentais pode alcançar simultaneamente a proteção material, no sentido de que os direitos fundamentais possuem natureza supralegal, estando no ápice do ordenamento; bem como a proteção formal, sujeitando estes direitos a limite de reforma constitucional, como cláusulas pétreas.

Não abarca, portanto, o pensamento jusnaturalista ou subjetivista do conteúdo destas normas. Afinal, seu fundamento possui previsão legal, inserta na grande maioria das constituições de origem romano-germânica. É exatamente o caso do Brasil.

No julgamento conjunto de Ações Diretas de Inconstitucionalidade movidas contra a Medida Provisória n. 954/2020, o Supremo Tribunal Federal, num movimento de ampliação e amparado no parágrafo segundo do art. 5º da Constituição Federal, reconheceu como fundamentais os direitos à proteção de dados e à autodeterminação informativa, o que veio a embasar recente reforma constitucional.



### 2.2.2 A Medida Provisória n. 954/2020 e o julgamento pelo STF

O avanço da tecnologia trouxe diversas transformações para a sociedade. Diante da acelerada e crescente comunicação de dados, mais do que nunca, faz-se necessário um sistema eficaz de proteção de dados.

Neste sentido, sobre a inovação decorrente da comunicação de dados, Ferraz Jr. (2020, p. 167) esclarece que:

A comunicação de dados representa uma inovação com meio sócio-histórico de comunicação. Ao começar pela expressão dados, expressão tornada usual e que traduz data em latim anglicizado. O termo é, em geral, usado no plural, talvez porque um dado isolado não tem nenhum valor, na medida em que não permite realizar operações sobre ele. Por característica, os dados são “expressos” por uma escritura numérica (algoritmos) que, para se manifestar como signos (sentido), exige uma prévia separação entre o suporte material e a significação, adquirindo um caráter próprio, que permite uma atividade, a combinatória binária, independente de toda e qualquer significação. Ao contrário da palavra grafada, telegrafada, telefonada, os dados surgem por essa atividade sem suporte material, portanto alheia ao espaço e ao tempo, que, mesmo quando é traduzida em textos, cores, sons, não passa de uma atividade combinatória muda e inexpressiva.

Dentro deste cenário, ganhou relevância para o estudo da matéria o julgamento das Ações Diretas de Inconstitucionalidade opostas contra a Medida Provisória n. 954/2020 (MP).

A referida MP foi editada no início da pandemia da COVID-19, no ano de 2020, e visava

[...] o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. (BRASIL. Supremo Tribunal Federal. Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.390. Relator: Ministro Rosa Weber. Plenário. Disponível em: [www.stf.jus.br](http://www.stf.jus.br). Acesso em: 4 ago. 2021).

Por apresentar uma série de vícios, a MP 954/2020 foi objeto de diversas Ações Diretas de Inconstitucionalidade, sendo que, no julgamento das referidas ações, foi reconhecido como fundamental o direito à proteção de dados e à autodeterminação informativa pelo Supremo Tribunal Federal.

Na decisão<sup>16</sup> foram tratados aspectos relacionados à inconstitucionalidade formal – pelo não atendimento dos requisitos de relevância e urgência (art. 62 da CF) – e da inconstitucionalidade material, com base na violação das “regras constitucionais da dignidade da pessoa humana, da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, do sigilo dos dados e da autodeterminação informativa, albergados nos arts. 1º, inciso III, e 5º, incisos X e XII da nossa Lei Fundamental”.

A Medida Provisória n. 954/2020 previa que:

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 62 da Constituição, adota a seguinte Medida Provisória, com força de lei:

Art. 1º Esta Medida Provisória dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras do Serviço Telefônico Fixo Comutado - STFC e do Serviço Móvel Pessoal - SMP com a Fundação Instituto Brasileiro de Geografia e Estatística - IBGE.

Parágrafo único. O disposto nesta Medida Provisória se aplica durante a situação de emergência de saúde pública de importância internacional decorrente do corona vírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020.

Art. 2º As empresas de telecomunicação prestadoras do STFC e do SMP deverão disponibilizar à Fundação IBGE, em meio eletrônico, a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas.

§ 1º Os dados de que trata o caput serão utilizados direta e exclusivamente pela Fundação IBGE para a produção estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares.

§ 2º Ato do Presidente da Fundação IBGE, ouvida a Agência Nacional de Telecomunicações, disporá, no prazo de três dias, contado da data de publicação desta Medida Provisória, sobre o procedimento para a disponibilização dos dados de que trata o caput.

§ 3º Os dados deverão ser disponibilizados no prazo de:

I - sete dias, contado da data de publicação do ato de que trata o § 2º; e

II - quatorze dias, contado da data da solicitação, para as solicitações subsequentes.

Art. 3º Os dados compartilhados:

I - terão caráter sigiloso;

II - serão usados exclusivamente para a finalidade prevista no § 1º do art. 2º; e

---

<sup>16</sup> Sobre a importância do julgamento da Medida Provisória n. 954/2020, pontuam Bulzico e Sousa (2022, fls. 155): “Portanto, nesse ponto a LGPD encontra-se diante do desafio de revisitar o alcance da publicidade dos processos judiciais eletrônicos para compatibilizá-la com a proteção de dados pessoais, também elevada ao *status* constitucional pelo STF que reconheceu o direito fundamental à autodeterminação informacional, em maio de 2020, mediante o julgamento da Medida Provisória n.º 954/2020. Essa Medida Provisória dispunha que as companhias telefônicas compartilhassem o nome, número telefônico e endereço dos seus clientes com o Instituto Brasileiro de Geografia e Estatística (IBGE) intencionado a permitir a adoção de políticas para o combate da pandemia do Covid-19 e reconstrução do país. No julgamento liminar, em 24 de abril de 2020, a relatora Ministra Rosa Weber considerou a norma abusiva e determinou a suspensão da Medida Provisória pois, além da imprecisão técnica, havia desproporcional impacto ao benefício social promovido, já que impunha a cessão de dados considerados desnecessários para a pesquisa, porém capazes de impactar massivamente os titulares desses dados.”

III - não serão utilizados como objeto de certidão ou meio de prova em processo administrativo, fiscal ou judicial, nos termos do disposto na Lei nº 5.534, de 14 de novembro de 1968.

§ 1º É vedado à Fundação IBGE disponibilizar os dados a que se refere o caput do art. 2º a quaisquer empresas públicas ou privadas ou a órgãos ou entidades da administração pública direta ou indireta de quaisquer dos entes federativos.

§ 2º A Fundação IBGE informará, em seu sítio eletrônico, as situações em que os dados referidos no caput do art. 2º foram utilizados e divulgará relatório de impacto à proteção de dados pessoais, nos termos do disposto na Lei nº 13.709, de 14 de agosto de 2018.

Art. 4º Superada a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), nos termos do disposto na Lei nº 13.979, de 2020, as informações compartilhadas na forma prevista no caput do art. 2º ou no art. 3º serão eliminadas das bases de dados da Fundação IBGE.

Parágrafo único. Na hipótese de necessidade de conclusão de produção estatística oficial, a Fundação IBGE poderá utilizar os dados pelo prazo de trinta dias, contado do fim da situação de emergência de saúde pública de importância internacional.

Art. 5º Esta Medida Provisória entra em vigor na data de sua publicação.

Foram cinco Ações Diretas de Inconstitucionalidade referentes à Medida Provisória n. 954/2020, distribuídas para a mesma relatora - Ministra Rosa Weber -, sendo a primeira ajuizada pelo Conselho Federal da OAB e as demais pelos partidos políticos PSDB, PSB, PSOL e PCdoB.

Dentre estas, o PSOL pediu que fosse declarada a inconstitucionalidade formal da referida medida provisória sob o fundamento de que o ato normativo não observava os requisitos da relevância e da urgência previstos no art. 62 da CF, bem como em razão da inconstitucionalidade material do dispositivo.

Tal partido político entendeu que o ato afrontava o direito fundamental à proteção de dados, que decorreria da conjugação das normas protetivas da dignidade da pessoa humana, da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, bem como do sigilo de dados, previstos no art. 5º, incisos X e XII da Constituição Federal.

O Conselho Federal da OAB pediu também que fosse reconhecido o:

[...] direito fundamental à autodeterminação informativa, a ensejar a tutela jurisdicional quando sua violação não for devidamente justificada por motivo suficiente, proporcional, necessário e adequado e com proteção efetiva do sigilo perante terceiros, com governança que inclua o Judiciário, o Ministério Público, a Advocacia e entidades da sociedade civil”. (BRASIL. Supremo Tribunal Federal. Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.390. Relator: Ministro Rosa Weber. Plenário, p. 6. Disponível em: [www.stf.jus.br](http://www.stf.jus.br). Acesso em: 4 ago. 2021.).

Preenchidos os requisitos legais, foi deferida medida cautelar monocraticamente pela Ministra Rosa Weber, que deveria ser referendada pelo Plenário do Supremo Tribunal Federal, para suspender a eficácia da aludida Medida Provisória, determinando que o Instituto Brasileiro de Geografia e Estatística (IBGE) se absteresse de requerer a disponibilização dos dados ou, caso já tivesse requerido, que sustasse o pedido.

Foi determinada, também, a tramitação conjunta do referido feito com as Ações Diretas de Inconstitucionalidade ns. 6387, 6388, 6389 e 6390, que também impugnaram a constitucionalidade da Medida Provisória n. 954/2020.

Na decisão sobre a medida cautelar foram tratados aspectos relacionados à inconstitucionalidade formal – pelo não atendimento dos requisitos de relevância e urgência (art. 62 da CF) – e da inconstitucionalidade material, com base na violação das:

regras constitucionais da dignidade da pessoa humana, da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, do sigilo dos dados e da autodeterminação informativa, albergados nos arts. 1º, inciso III, e 5º, incisos X e XII da nossa Lei Fundamental.

A ementa da decisão sintetizou os seus fundamentos, a saber:

MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE. REFERENDO. MEDIDA PROVISÓRIA Nº 954/2020. EMERGÊNCIA DE SAÚDE PÚBLICA DE IMPORTÂNCIA INTERNACIONAL DECORRENTE DO NOVO CORONAVÍRUS (COVID-19). COMPARTILHAMENTO DE DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO FIXO COMUTADO E DO SERVIÇO MÓVEL PESSOAL, PELAS EMPRESAS PRESTADORAS, COM O INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. *FUMUS BONI JURIS. PERICULUM IN MORA*. DEFERIMENTO.

1. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais.

2. Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais não de observar os limites delineados pelo 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), sob pena de lesão a esses direitos. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados [...].

6. Ao não apresentar mecanismo técnico ou administrativo apto a proteger, de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão, seja no tratamento, o sigilo, a higidez e, quando o caso, o anonimato dos dados

peçoais compartilhados, a MP nº 954/2020 descumpra as exigências que exsurtem do texto constitucional no tocante à efetiva proteção dos direitos fundamentais dos brasileiros [...].

10. *Fumus boni juris e periculum in mora* demonstrados. Deferimento da medida cautelar para suspender a eficácia da Medida Provisória nº 954/2020, a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel.

11. Medida cautelar referendada. (BRASIL. Supremo Tribunal Federal. Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.390. Relator: Ministro Rosa Weber. Plenário, p. 1. Disponível em: [www.stf.jus.br](http://www.stf.jus.br). Acesso em: 4 ago. 2021).

Neste particular, reconhecendo os desafios relacionados à temática, merece destaque os seguintes trechos do voto da Ministra Relatora:

14. Entendo que as condições em que se dá a manipulação de dados pessoais digitalizados, por agentes públicos ou privados, consiste em um dos maiores desafios contemporâneos do direito à privacidade.

A Constituição da República confere especial proteção à intimidade, à vida privada, à honra e à imagem das pessoas ao qualificá-las como invioláveis, enquanto direitos fundamentais da personalidade, assegurando indenização pelo dano material ou moral decorrente de sua violação (art. 5º, X). O assim chamado direito à privacidade (*righttoprivacy*) e os seus consectários direitos à intimidade, à honra e à imagem emanam do reconhecimento de que a personalidade individual merece ser protegida em todas as suas manifestações.[...].

Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais. (BRASIL. Supremo Tribunal Federal. Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.390. Relator: Ministro Rosa Weber. Plenário, p. 15-16. Disponível em: [www.stf.jus.br](http://www.stf.jus.br). Acesso em: 4 ago. 2021).

Na mesma linha, o Ministro Luiz Fux (p. 49)<sup>17</sup> asseverou que “a proteção de dados pessoais e autodeterminação informativa são direitos fundamentais autônomos extraídos da garantia da inviolabilidade da intimidade e da vida privada e, consectariamente, do princípio da dignidade da pessoa humana”.

Já o Ministro Gilmar Mendes, no referido julgamento, destacou que:

Na doutrina pátria, o reconhecimento da autonomia do direito fundamental à proteção de dados foi desenvolvido em termos dogmáticos a partir das importantes

<sup>17</sup> Para Mendes, Rodrigues Jr. e Fonseca (2021, p. 67): “Não por acaso, o Ministro Luiz Fux destacou a centralidade do tema da proteção de dados em face da manutenção da democracia, uma vez que dados aparentemente “insignificantes” podem ser utilizados até mesmo para distorcer processos eleitorais. “(o) recente escândalo envolvendo a Cambridge Analytica revelou como modelos de negócios são rentabilizados pela análise de dados e alertou como seu uso indevido pode lesar (...) a própria democracia””.

contribuições da Professora Laura Schertel Mendes. Nas palavras da autora, entende-se que:

“Para além da coincidência do léxico com os modernos instrumentos internacionais de tutela da privacidade, certo é que a proteção da dignidade humana e a inviolabilidade da intimidade e da vida privada numa sociedade da informação somente pode ser atingida hoje por meio da proteção contra os riscos do processamento de dados pessoais. Assim, quando se interpreta a norma do art. 5º, X, em conjunto com a garantia do *habeas data* e com o princípio fundamental da dignidade humana, é possível extrair-se da Constituição Federal um verdadeiro direito fundamental à proteção de dados pessoais.

Entendemos que o reconhecimento desse direito fundamental não é apenas uma possibilidade; trata-se de uma necessidade para tornar efetivos os fundamentos e princípios do Estado democrático de direito, na sociedade contemporânea da informação, conforme determina a Constituição Federal” (MENDES, Laura Schertel Ferreira. *Habeas data e autodeterminação informativa: os dois lados da mesma moeda*. Direitos Fundamentais & Justiça, Belo Horizonte, ano 12, n. 39, p. 185-216, jul./dez. 2018. p. 188).

A afirmação da autonomia do direito fundamental à proteção de dados pessoais – há de se dizer – não se faz tributária de mero encantamento teórico, mas antes da necessidade inafastável de afirmação de direitos fundamentais nas sociedades democráticas contemporâneas.

Considerando que os espaços digitais são controlados por agentes econômicos dotados de alta capacidade de coleta, armazenamento e processamento de dados pessoais, a intensificação do fluxo comunicacional na internet aumenta as possibilidades de violação de direitos de personalidade e de privacidade.

Todas essas transformações tecnológicas ensejam aquilo que, nas palavras de Bruno Bioni, é identificado como verdadeiro *cenário de hipervulnerabilidade no regime de proteção de dados pessoais*, que se desdobra em traços vulnerantes peculiares sob as perspectivas informacional, técnica e econômica (BIONI, op. cit., p. 164).

Desse modo, a afirmação da força normativa do direito fundamental à proteção de dados pessoais decorre da necessidade indissociável de proteção à dignidade da pessoa humana ante a contínua exposição dos indivíduos aos riscos de comprometimento da autodeterminação informacional nas sociedades contemporâneas.

É importante ainda assentar que essa afirmação de um novo direito fundamental não resulta de um criacionismo jurisprudencial dissociado da própria tradição jurídica brasileira, naquilo que transformada pelos recentes influxos legislativos.

A privacidade somente poderia ser relativizada, portanto, diante de justificativa consistente e legítima, o que não se observava no texto da mencionada medida provisória, não tendo sido demonstrado qual seria o interesse público no compartilhamento dos dados pessoais, consideradas a suposta necessidade<sup>18</sup>, adequação e proporcionalidade da medida.

<sup>18</sup> No relatório da análise realizada sobre o tratamento de dados pessoais na consulta de jurisprudência, pontuou o CNJ (2021, p. 11) que: “Em termos mais concretos, 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 microsistema de proteção de dados, para 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. Essa autorização, no entanto, não deve ser entendida como uma carta branca para a irrestrita divulgação de informações judiciais sobre pessoas naturais. Isso porque, embora seja legítima e dispense consentimento, a 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

Como esta medida provisória não apontava, efetivamente, o modo e a finalidade dos dados coletados, sequer oferecia condições para a aferição dos referidos elementos.

Diante da colisão de interesses, e analisando com base na proporcionalidade, a questão sobre a desnecessidade ficou evidenciada também pelo fato de que o próprio IBGE anunciou, segundo o julgado, que teria viabilizado o início da pesquisa por meio da base de 211 (duzentos e onze) mil domicílios que haviam participado da Pesquisa Nacional por Amostra de Domicílios Contínua (PNAD) no primeiro trimestre de 2019, tendo selecionado aqueles que possuíam número de telefone cadastrado.

A análise da proporcionalidade também restou comprometida pela ausência de estipulação na Medida Provisória de providências para a anonimização ou pseudoanonimização dos dados, diante da necessidade de se assegurar a liberdade individual, tendo ainda frisado a Ministra Relatora, diante da postergação do início da vigência naquela época da Lei Geral de Proteção de Dados, que:

O que explicito, neste juízo perfunctório, é que não se pode fazê-lo de uma forma que não garanta mecanismos de proteção compatíveis com as cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, *caput*), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII).

Assim como o exigir que automóveis sejam providos de freios, *airbags* e espelhos retrovisores não significa criar obstáculos para a indústria automobilística, o exigir que normas que envolvam direitos fundamentais e da personalidade observem requisitos mínimos de adequação constitucional tampouco pode ser lido como embaraço à atividade estatal. (BRASIL. Supremo Tribunal Federal. Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.390. Relator: Ministro Rosa Weber. Plenário, p. 23. Disponível em [www.stf.jus.br](http://www.stf.jus.br). Acesso em: 4 ago. 2021.)

O voto do Ministro Edson Fachin também abordou a questão da proteção de dados e da autodeterminação afirmativa, ao sustentar que

---

responsabilização e prestação de contas (art. 6º). Nesse contexto, especial destaque merece o princípio da necessidade, que, na definição da LGPD, prescreve a “limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados” (art. 6º, III). Em outras palavras: ainda quando justificado, o tratamento dos dados deve se ater aos limites do estritamente necessário para atingir a finalidade que o justifica. Aplicado à prática judiciária, o princípio da necessidade deve nortear o processo de redação de manifestações dos(as) magistrados(as) durante o processo de redação de suas manifestações. Na elaboração de despachos, decisões, sentenças, relatórios, votos, ementas e textos congêneres, impõe-se aos juízes e às juízas a cautela de omitir ou pseudonimizar dados pessoais cuja publicização seja dispensável”.

[...] no caso concreto, nem a excepcionalidade da crise vivida, nem a valorosa tarefa de produzir estudos estatísticos justifica a violação dos direitos fundamentais dos usuários dos serviços de telefonia à intimidade, ao sigilo e à autonomia informativa. (BRASIL. Supremo Tribunal Federal. Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.390. Relator: Ministro Rosa Weber. Plenário, p. 38. Disponível em: [www.stf.jus.br](http://www.stf.jus.br). Acesso em: 4 ago. 2021).

Na mesma linha, o Ministro Luiz Fux (p. 49) asseverou que “a proteção de dados pessoais e autodeterminação informativa são direitos fundamentais autônomos extraídos da garantia da inviolabilidade da intimidade e da vida privada e, conseqüentemente, do princípio da dignidade da pessoa humana”. E complementou:

Exatamente por isso tudo, no meu modo de ver, a Medida Provisória nº 954/2020 ultrapassa todos os limites fixados pelos direitos fundamentais à proteção de dados, à autodeterminação informativa e à privacidade, inobservando ainda o postulado da proporcionalidade, mormente porque não delimita o objeto e incorre em excesso ao determinar o compartilhamento de dados de milhões de brasileiros, quando as pesquisas amostrais realizadas pelo IBGE, em geral, envolvem apenas 70 mil pessoas. Então, é absolutamente um tratamento imoderado, irrazoável e que não merece a chancela da Suprema Corte. (BRASIL. Supremo Tribunal Federal. Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.390. Relator: Ministro Rosa Weber. Plenário, p. 49. Disponível em: [www.stf.jus.br](http://www.stf.jus.br). Acesso em: 4 ago. 2021).

Em relação ao tema, o Ministro Gilmar Mendes pontuou, em seu voto, que:

O quadro fático contemporâneo deve ser internalizado na leitura e aplicação da Constituição Federal de 1988. Aliás, ousaria a dizer que nunca foi estranha à jurisdição constitucional a ideia de que os parâmetros de proteção dos direitos fundamentais devem ser permanentemente abertos à evolução tecnológica. Dentro da tradição do *judicial review* norte-americano, por exemplo, mesmo partidários de uma interpretação originalista da Constituição reconhecem que a inovação naturalmente levanta questões sobre como a Constituição a ela se aplica. (BRASIL. Supremo Tribunal Federal. Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.390. Relator: Ministro Rosa Weber. Plenário, p. 95. Disponível em: [www.stf.jus.br](http://www.stf.jus.br). Acesso em: 4 ago. 2021).

Ademais, sustentou o Ministro Gilmar Mendes que:

O direito fundamental à proteção de dados pessoais nos contornos aqui assinalados não assume natureza absoluta, mas, como qualquer outro direito fundamental, admite flexibilizações, traduzidas na possibilidade concreta de uso e tratamento desses dados para a realização de finalidades de interesse público legitimamente protegidas pelo ordenamento jurídico.

No caso em tela, contudo, fazendo incidir os parâmetros de tutela do direito à autodeterminação informacional, verifica-se que a Medida Provisória 954/2020 é



altamente deficitária na fixação de salvaguardas mínimas para a garantia da privacidade dos usuários de serviços de telefonia no Brasil. (BRASIL. Supremo Tribunal Federal. Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.390. Relator: Ministro Rosa Weber. Plenário, p. 110. Disponível em [www.stf.jus.br](http://www.stf.jus.br); Acesso em 4 ago. 2021).

Diante da identificação dos aspectos materiais da fundamentalidade, com menção expressa ao Estado Democrático de Direito e à Dignidade da Pessoa Humana, o reconhecimento ao direito subjetivo à proteção de dados e a autodeterminação informativa<sup>19</sup> representa a renovação da proteção constitucional à privacidade<sup>20</sup> e ao sigilo de dados diante das novas ameaças decorrentes da evolução tecnológica.

Inclusive, sobre o direito à privacidade e à proteção de dados, Aranha e Ferreira (2020, p. 2) sinalizam que, em que pese tutelem valores parecidos, a saber, a autonomia e a dignidade dos indivíduos, bem como o desenvolvimento livre da personalidade, pensamento e opiniões, os referidos direitos se diferenciam quanto à utilização e o escopo.

Ademais, pontuam Mendes, Rodrigues Jr. e Fonseca (2021, p. 67) :

Segundo o Ministro Gilmar Mendes, o conteúdo desse direito fundamental exorbita àquele protegido pelo direito à privacidade, pois não se limita apenas aos dados íntimos ou privados. Ao contrário, refere-se a qualquer dado que identifique ou possa identificar um indivíduo. Esse direito fundamental autônomo e com contornos próprios, seria extraído de uma: “Compreensão integrada do texto constitucional lastreada (i) no direito fundamental à dignidade humana, (ii) na concretização do compromisso permanente de renovação da força normativa da proteção constitucional à intimidade (art. 5º, inciso X, da CF/88) diante do espraiamento de novos riscos derivados do avanço tecnológico e ainda (iii) no reconhecimento da centralidade do *habeas data* enquanto instrumento de tutela materiais do direito à autodeterminação informativa”.

O reconhecimento do direito fundamental à proteção de dados pessoais representa, efetivamente, um grande avanço à tutela da personalidade.

---

<sup>19</sup> Para Mendes, Rodrigues Jr. e Fonseca (2021, p. 69): “Com isso, a autonomia do direito fundamental à proteção de dados pessoais, também designado por alguns ministros como o direito à autodeterminação informativa, permite que se formule uma diferenciação entre a inviolabilidade da intimidade e da vida privada e a proteção de dados. Tem-se, portanto, um passo fundamental para a proteção da personalidade dos cidadãos na sociedade da informação”.

<sup>20</sup> Neste particular, Mendes e Fonseca (2021, p. 76-77) destacam: “Nesse contexto, muitas das discussões regulatórias começaram a se referir ao direito à proteção de dados pessoais, concebido para além de uma mera decorrência da privacidade: um direito fundamental autônomo cujo âmbito de proteção está vinculado à tutela da dignidade e da personalidade dos cidadãos no seio da sociedade da informação”.

E, nesta linha, destacam Mendes, Rodrigues Jr. e Fonseca (2021, p. 68):

Quanto aos efeitos gerados por essa proteção, amoldando-a ao conceito de autodeterminação informativa, é possível pensá-los a partir de uma dupla dimensão. De um lado, (a) essa proteção se desdobra como liberdade negativa do cidadão, oponível diante do Estado, demarcando seu espaço individual de não intervenção estatal (dimensão subjetiva). De outro, (b) ela estabelece um dever de atuação estatal protetiva no sentido de estabelecer condições e procedimentos aptos a garantir o exercício e a fruição desse direito fundamental (dimensão objetiva).

A Medida Provisória impugnada por meio das referidas ADINS não veio a ser convertida em lei no prazo previsto pela Constituição Federal, tendo sua vigência expirado em 14 de agosto de 2020 e, por consequência, as Ações Diretas de Inconstitucionalidades foram julgadas prejudicadas por perda superveniente do seu objeto.

Em situações como esta, a jurisprudência do Supremo Tribunal Federal é consolidada no sentido de que a extinção da vigência da norma, após o ajuizamento da ADIN, implica perda superveniente do seu objeto.

Com isto, as ADINS foram julgadas prejudicadas por perda superveniente do seu objeto, tendo sido proferida decisão de extinção dos processos sem resolução do mérito, que já transitou em julgado.

No entanto, por meio da decisão sobre o referendo da medida cautelar<sup>21</sup>, o STF reconheceu como direitos fundamentais o direito à proteção de dados e à autodeterminação informativa<sup>22</sup>, que não estavam previstos expressamente no rol elencado na Constituição

---

<sup>21</sup> Lembram Longhi e Martins (2020, p. 3) que: “Hipótese semelhante já foi julgada pela Corte Constitucional alemã. Em 1983, o reconhecimento do direito fundamental à autodeterminação informativa (informationelles Selbstbestimmung) pelo Tribunal Constitucional Alemão (Bundesverfassungsgericht – TCA) foi mais um episódio desse atrito. No conhecido julgamento sobre a Lei do Censo (Volkszählungsurteil – 1 BvR 209/83, de 15.02.83) foi discutida a constitucionalidade de uma lei federal que permitia a coleta e tratamento de dados para fins estatísticos, bem como a transmissão anonimizada desses dados para a execução de atividades públicas. Os juízes do TCA entenderam que a lei era parcialmente constitucional. Seria constitucional a permissão para a coleta e tratamento de dados pessoais dos cidadãos, independente do seu consentimento, bastando a permissão legal. Entretanto, a permissão geral dada pela lei de comparação e troca de dados pessoais entre órgãos públicos, bem como a fixação de competência, foi considerada inconstitucional, por violar o princípio da autodeterminação informativa. O reconhecimento desse novo direito fundamental decorreu de uma interpretação do direito de personalidade e da dignidade da pessoa humana. O ponto central da discussão era a transparência do tratamento dos dados pessoais. Sem que a lei fixe de forma clara como os dados serão tratados, os cidadãos, obrigados a entregarem suas informações pessoais, não poderiam saber quem teria acesso e para quais finalidades seriam utilizados, vivendo uma situação de constante vigilância. A autodeterminação informativa, dessa forma, não estaria ligada ao controle total do titular sobre o tratamento de seus dados, mas de poder verificar a legalidade das atividades daqueles que utilizam seus dados, independentemente do consentimento”.

<sup>22</sup> Neste sentido, ponderam Mendes e Fonseca (2021, p. 91): “Nesse contexto, a garantia da autodeterminação informativa continua a ser importante objetivo da proteção de dados pessoais. Essa autodeterminação, contudo,

Federal, mas que possuíam fundamentalidade, e que podem ser extraídos da proteção à intimidade e à vida privada (art. 5º, X, CF/88), e do princípio da dignidade da pessoa humana (art. 1º, III, CF/88) e da garantia processual do habeas data (BRASIL, CF, 1988, art. 5º, LXXII).

Posteriormente, por meio da Emenda Constitucional de número 115, em 2022, foi inserido o inciso LXXIX no artigo 5º da Constitucional Federal, que dispõe: “é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais”<sup>23</sup>, explicitando direito que antes já decorria das inviolabilidades previstas na Constituição (BRASIL, 2022).

### 2.3 A LEI GERAL DE PROTEÇÃO DE DADOS

A Lei de n. 13.709 de 2018 (LGPD), como já destacado, instituiu o sistema de proteção de dados no Brasil<sup>24</sup>. No âmbito interno, a questão da proteção dos dados pessoais nos processos judiciais vem ganhando relevância, num momento de acelerado avanço da tecnologia.

---

somente pode ser concretizada quando considerados os limites resultantes do fenômeno da informação e de contextos sociais que muitas vezes impossibilitam a tomada de uma decisão livre pelo indivíduo. Uma proteção de dados pessoais efetiva precisa ir além da garantia meramente formal do consentimento individual. É preciso assegurar os pressupostos materiais dessa proteção para se construir um espaço de liberdade no qual o indivíduo esteja apto a configurar as suas relações informacionais”.

<sup>23</sup> No entanto, advertem Mendes, Rodrigues Jr. e Fonseca (2021, p. 69): “A despeito das construções desenvolvidas nas seções anteriores, não se pode conceber o direito à proteção de dados de forma absoluta. As informações pessoais não são apenas titularidades individuais. Elas integram a órbita de sua representação no corpo social, o que demanda escolhas feitas em lei ou na Constituição, que demandem seu processamento ou sua exposição. A limitação desse direito fundamental, no caso concreto, exige, (i) uma base jurídica segura, (ii) com a clareza necessária sobre a finalidade do tratamento de dados, para que se avalie o nível de intervenção no direito fundamental, (iii) e que seja também proporcional, adequada e necessária à finalidade pretendida, adotando, ainda, (iv) as providências preventivas mínimas de cunho procedimental e organizacional, orientadas à segurança dos cidadãos envolvidos e à diminuição dos riscos de danos a seus direitos da personalidade. Em verdade, quanto mais grave for essa restrição, mais contundentes devem ser as justificativas, os critérios e as precauções para tal fim, sob pena de se legitimar intervenções na vida privada em nome de fins genéricos ou necessidades coletivas abstratas. O amplo acesso aos dados pessoais dos cidadãos brasileiros exige, no mínimo, balizas legislativas em relação a essa coleta ou transferência, a partir da previsão de medidas e de critérios de intervenção proporcionais à gravidade da restrição a esse direito fundamental”.

<sup>24</sup> No relatório da análise realizada sobre o tratamento de dados pessoais na consulta de jurisprudência, pontuou o CNJ (2021, p. 7) que: “A Lei Geral de Proteção de Dados Pessoais surge como uma resposta do ordenamento jurídico brasileiro às profundas transformações sociais causadas pela evolução das tecnologias de armazenamento, compartilhamento e processamento de dados. 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. Especificamente

A LGPD constitui-se uma norma importante e que trata de temática que vem sendo enfrentada por muitos países na atualidade<sup>25</sup>.

Em toda operação de tratamento, a referida lei impõe que sejam observadas, em especial, a boa-fé, a finalidade, não sendo admitida a possibilidade de realização posterior de outro tratamento sem que seja respeitada a finalidade. É necessário que seja observada a responsabilidade, bem como a prestação de contas, numa postura que deve ser transparente, resguardando a vida privada e a intimidade.

A LGPD estabeleceu, em seus artigos primeiro e segundo, quais seriam o objeto e os fundamentos da disciplina da proteção de dados pessoais, a saber:

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios.

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

- I - o respeito à privacidade;
- II - a autodeterminação informativa;
- III - a liberdade de expressão, de informação, de comunicação e de opinião;
- IV - a inviolabilidade da intimidade, da honra e da imagem;
- V - o desenvolvimento econômico e tecnológico e a inovação;
- VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

---

no âmbito do Poder Judiciário, a transformação digital tem se concretizado paulatinamente, desde os anos 1990, a partir com base em 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)”.

<sup>25</sup> Sobre a importância da LGPD, pondera Teffé (2022, p. 55): “No presente cenário, verifica-se que tanto instituições quanto estudiosos da temática dos dados pessoais sensíveis vêm levantando três importantes questões: (a) diante do avanço tecnológico e do contexto da hiperconectividade, mais e mais dados vêm sendo compreendidos como pessoais, ou seja, vinculados direta ou indiretamente a indivíduos identificados ou identificáveis; (b) há cada vez mais formas de análises que podem identificar indivíduos e revelar dados sensíveis sobre eles; e (c) não obstante a proximidade entre os textos legais do GDPR e da LGPD, já pontos específicos de diferenças entre as normas, bem como legislação setorial diversa, não sendo possível importar sempre e diretamente interpretações europeias para o cenário brasileiro. Assim, ainda que o estudo da norma europeia seja fundamental e represente base inicial para se analisar a LGPD, mostra-se essencial o desenvolvimento de documentos institucionais e de doutrina que expressem e interpretem amplamente o contexto brasileiro de proteção de dados”.

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (BRASIL, 2018).

Nos termos do seu art. 1º, a LGPD é responsável por disciplinar o tratamento de dados pessoais, tanto nos meios físicos quanto nos meios digitais, realizado por pessoa física ou jurídica, tanto do direito público quanto do direito privado, com o objetivo de “proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (BRASIL, 2018).

Não existem dúvidas de que a LGPD deve ser observada quando do tratamento de dados pessoais por pessoa jurídica de direito público e que esta visa proteger o direito fundamental da liberdade, da privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A LGPD não incide em algumas hipóteses de tratamentos de dados, descritas no seu art. 4º, que inclui aqueles realizados por pessoa natural para fins particulares (não econômicos), realizados com finalidade jornalística e artística, acadêmica, de segurança nacional, de defesa nacional, de segurança do Estado, de atividades de investigação e repressão de infrações penais ou em hipóteses de tratamento fora do território, sem compartilhamento com agentes brasileiros ou objeto de transferência internacional.

A LGPD elencou, dentre outros, a autodeterminação informativa, o respeito à privacidade e a inviolabilidade da intimidade como fundamentos para a proteção de dados pessoais.

Desse modo, percebe-se que esta Lei é um reforço, no sistema jurídico, para a questão da privacidade sob a ótica da proteção dos dados.

A importância da LGPD, na atualidade, é destacada por Cueva (2020, p. 200):

A LGPD, contudo, disciplina de maneira sistemática e coerente a coleta, o armazenamento, o tratamento e a disseminação de dados pessoais, que constituem o principal insumo da economia digital para a formação de perfis informacionais, mediante a precisa identificação de hábitos, preferências e decisões existenciais e políticas dos titulares de dados.

A Lei Geral de Proteção de Dados, Lei n. 13.709/2018<sup>26</sup>, interage com o Marco Civil da Internet, Lei n. 12.965 de 2014, tendo promovido alterações no referido dispositivo normativo, sendo que a LGPD tutela a proteção de dados pessoais nas relações jurídica de uma forma geral e o Marco Civil da Internet trata de dados pessoais nas relações que dependam do uso da internet.

Destaca-se, ainda, que a proteção de dados pessoais também encontra regulamentação no Código de Defesa do Consumidor (CDC) e na Lei de Acesso à Informação (LAI)<sup>27 28</sup>, dentre outras, em disciplinas relacionadas ao microsistema instituído.

#### 2.4 DADOS PESSOAIS E DADOS PESSOAIS SENSÍVEIS

Na atualidade, os dados pessoais são bens de elevado valor e importância, sendo a mola propulsora da revolução digital e da inteligência artificial.

Nesta nova realidade, Negrão (2020, p. 30) pondera que a necessidade de elaboração de marcos regulatórios decorreu da utilização crescente e da manipulação de dados pessoais para

---

<sup>26</sup> Com a promulgação da LGPD, foi editada pelo CNJ a Resolução n. 363, em 12 de janeiro de 2024, que estabelecia medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais.

<sup>27</sup> Conforme Enunciado 688 do Conselho da Justiça Federal: “A Lei de Acesso à Informação (LAI) e a Lei Geral de Proteção de Dados Pessoais (LGPD) estabelecem sistemas compatíveis de gestão e proteção de dados. A LGPD não afasta a publicidade e o acesso à informação nos termos da LAI, amparando-se nas bases legais do art. 7º, II ou III, e art. 11, II, a ou b, da Lei Geral de Proteção de Dados”.

<sup>28</sup> Sobre a relação da LAI com a LGPD, destaca Santos (2021, p.101) que: “A Lei de Acesso à Informação, Lei n.º 12.527/2011 (BRASIL), cita em seu artigo 1º, o inciso II, do §3º do art. 37 da Constituição Federal o qual determina o acesso dos usuários a registros administrativos e a informações sobre atos de governo, observado o disposto no art. 5º, X (são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação) e XXXIII (todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado). Inclusive, a Lei de Acesso à Informação vem para regulamentar o inciso XXXIII, do art. 5º da Constituição Federal de 1988 (BRASIL). Assim, no primeiro momento tem-se o que, aparentemente, seria um conflito entre a publicidade, determinada pela Constituição Federal e regulamentada pela Lei de Acesso à Informação, e a proteção de dados, determinada pela LGPD”.

preservar a privacidade, especialmente, em razão da possibilidade de remuneração econômica decorrente da cessão de dados.

Sobre o conceito do que seria um “dado”, esclarece Ferraz Jr. (2020, p. 167-168):

A comunicação de dados representa uma inovação com meio sócio-histórico de comunicação. Ao começar pela expressão dados, expressão tornada usual e que traduz data em latim anglicizado. O termo é, em geral, usado no plural, talvez porque um dado isolado não tem nenhum valor, na medida em que não permite realizar operações sobre ele. Por característica, os dados são “expressos” por uma escritura numérica (algoritmos) que, para se manifestar como signos (sentido), exige uma prévia separação entre o suporte material e a significação, adquirindo um caráter próprio, que permite uma atividade, a combinatória binária, independente de toda e qualquer significação. Ao contrário da palavra grafada, telegrafada, telefonada, os dados surgem por essa atividade sem suporte material, portanto alheia ao espaço e ao tempo, que, mesmo quando é traduzida em textos, cores, sons, não passa de uma atividade combinatória muda e inexpressiva [...].

No campo dos dados, diante da inexistência de limitação física, lidamos, pois, com bens, cujo uso por alguém não exclui, por princípio, o uso por outro. De fato, chega mesmo a ser conceitualmente impossível delimitar esse “alguém”. Nem mesmo como um sujeito coletivo”. O chamado ciberespaço somente se constrói na medida em cada espaço de ação de cada sujeito é voltado para a comunicação com os outros, sem a qual o próprio ambiente perde sentido. Vale dizer, altera-se a noção de *meio ambiente*, pois o meio e o ambiente se confundem.

Partindo desta premissa, a LGPD, em seu art. 5º, conceitua o que seria considerado como “dado pessoal” e “dado pessoal sensível” para efeitos da referida lei.<sup>29</sup> Nos termos do inciso I, o “dado pessoal” é aquela “informação relacionada à pessoa natural identificada ou identificável” (BRASIL, 2018).

Já o inciso II prevê que o “dado pessoal sensível” é o “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, quanto vinculado a uma pessoa natural” (BRASIL, 2018).

O artigo 7º da LGPD prevê hipóteses em que se permite o tratamento dos dados pessoais, que incluem o consentimento do titular, o cumprimento de obrigação legal e regulatória, para

---

<sup>29</sup> Neste sentido, pontuam Dirscherl e Faleiros Junior que (2024, p. 1): “O Regulamento Geral sobre a Proteção de Dados Pessoais da União Europeia (2016/679(EU)) também é importante marco normativo para o tema, pois define dados pessoais como informações que identificam ou são potencialmente identificáveis de um indivíduo. Já a legislação brasileira vai além, pois apresenta uma diferenciação entre dados pessoais e dados pessoais sensíveis, reconhecendo estes últimos como informações que, pelo que se pode inferir de seu rol enunciativo (art. 5º, II), podem revelar aspectos íntimos da vida”.

execução de políticas públicas e realização de estudos, para execução de contratos ou procedimentos preliminares relacionados a contrato, para proteção da vida e da incolumidade física do titular, para tutela da saúde, para proteção de crédito, quando necessário para atender a interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção de dados pessoais.

O inciso VI, do art. 7º, da LGPD, ainda prevê que o tratamento de dados pessoais poderá ser realizado para o exercício regular de direitos em processo judicial, administrativo ou arbitral, sendo que o tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram a sua disponibilização e que é dispensada a exigência do consentimento previsto para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e princípios desta lei.

Em ambos os casos, poderá haver novo tratamento de dados pessoais para novas finalidades, desde que observados os propósitos legítimos e específicos deste novo tratamento e os direitos do titular, assim como os ditames da LGPD.

Por envolver temas relacionados à intimidade da pessoa natural, a referida lei prevê um regime diferenciado para o tratamento dos dados pessoais sensíveis em seu artigo 11º, que assinala:

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

- a) cumprimento de obrigação legal ou regulatória pelo controlador;
- b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
- c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
- d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
- e) proteção da vida ou da incolumidade física do titular ou de terceiro;
- f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
- g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.



§ 2º Nos casos de aplicação do disposto nas alíneas “a” e “b” do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.

§ 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.

§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir:

I - a portabilidade de dados quando solicitada pelo titular; ou

II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo.

§ 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários (BRASIL, 2018).

As hipóteses previstas contemplam o consentimento vinculado à finalidade específica, ao cumprimento de obrigação legal ou regulatória, execução de políticas públicas, realização de estudos por órgão de pesquisa, garantindo a anonimização<sup>30</sup> dos dados quando possível, exercício regular de direitos, inclusive em contrato e em processo - administrativo, judicial e arbitral -, proteção da vida e integridade física do titular e terceiro, tutela da saúde, garantia da prevenção à fraude e segurança do titular em identificação e autenticação de cadastro em sistema eletrônico.

Sobre o tema, Teffé (2022, p. 39-45) adverte que:

Como apresentado, não se mostra possível definir, antecipadamente e de forma absoluta e permanente, os efeitos concretos de um tratamento de informações

---

<sup>30</sup> O Conselho Superior da Magistratura de Portugal, em parecer para fixação de critérios de seleção, tratamento, apresentação e arquivo de decisões judiciais na base de dados de tratamento de informação legal – já que nem todas as decisões são publicadas -, pontua que, em relação a anonimização (PORTUGAL, 2021): “Deve ser realizada a enumeração dos dados pessoais que sejam anonimizados, por razões de consistência e certeza jurídica. A enumeração deve, contudo, deixar espaço para anonimização adicional de outros dados, que normalmente por si só não permitem a identificação pessoal, mas em certos casos podem contribuir para a mesma. No que respeita aos métodos de anonimização, deve ser evitada a eliminação ou substituição total por pontos ou outros caracteres os dados pessoais, pois este método de anonimização dificulta a compreensão do texto. Quando sejam utilizadas iniciais, as mesmas devem ser utilizadas de modo aleatório, uma vez que o uso de iniciais com correspondência com o nome dos intervenientes processuais aumenta o risco de identificação de tais intervenientes. A anonimização deve ter sempre presente o necessário equilíbrio entre os interesses privados e públicos, o que significa que, para casos especiais, deve sempre existir a possibilidade de desvio das regras de anonimização estabelecidas, o que implica a assunção da decisão de não publicação de uma decisão sempre que se conclua que a aplicação das regras definidas de anonimização será insuficiente”.

personais, as intenções dos agentes de tratamento nem a real sensibilidade de um dado. Por exemplo, dados pessoais que pareçam não relevantes em determinado momento, que não façam referência a alguém diretamente ou, ainda, que não sejam formalmente sensíveis, uma vez transferidos, cruzados e/ou organizados, podem resultar em dados bastante específicos sobre determinada pessoa, trazendo informações, inclusive, de caráter sensível sobre ela. (...).

Ainda sobre informações que podem ser inseridas em tratamentos sensíveis, vale lembrar o histórico de compras de uma pessoa em um supermercado ou em uma farmácia ou o acesso à fatura de seu cartão de crédito, uma vez que, a partir disso, seria possível inferir dados sensíveis, como convicções religiosas, estado de saúde ou orientação sexual. Dados de geolocalização podem, também, ser manipulados para usos lesivos e discriminatórios em face do seu titular, permitindo ainda a verificação de informações sensíveis. Eles podem revelar, por exemplo, sua religião (pessoa localizada em determinado templo religioso) ou permitir que seja presumida alguma condição de saúde (pessoa localizada em uma clínica de saúde especializada em determinada doença). O CEP do domicílio de uma pessoa natural apresenta a potencialidade de ser utilizado para se analisar o padrão de vida e renda dela, assim como a profissão e eventual especialização acadêmica podem ajudar a inferir a renda média do sujeito. O próprio dado relativo à identidade de gênero – entendido dentro de um contexto amplo – por vezes é utilizado para discriminações ilícitas ou abusivas (...).

Isso sugere que a distinção entre dados pessoais gerais e dados pessoais sensíveis seria fundamentalmente falha, pelo menos quando usada para controlar a coleta de dados pessoais. Na era de análise de Big Data, essa distinção torna-se cada vez mais fluída, pois aparentemente qualquer dado pode se tornar sensível, se for encontrada uma maneira de, a partir, dele, serem inferidas informações sobre atributos assim protegidos.

Este estudo parte do pressuposto de que a LGPD lista quais são os dados que são de natureza sensível.

Ademais, existem dados que são tornados públicos pelo titular e dados de acesso público, que foram disponibilizados não pelo titular, mas sim por terceiros. Destaca-se, por oportuno, que um dado pessoal, mesmo tendo sido publicizado, continua tendo a natureza de pessoal, refletindo o direito de personalidade do seu titular. Pode ser transferido o direito de uso<sup>31</sup>, mas nunca o dado em si, pois o direito de personalidade é intransmissível.

Nesta linha, o tratamento destes dados deve sempre salvaguardar a liberdade, a privacidade e o livre desenvolvimento da personalidade nos termos do inciso IX, do art. 7º, da LGPD.

---

<sup>31</sup> Neste sentido, pontuam Doneda e Machado (2021, p. 331): “O fato de a Administração Pública possuir certos dados não significa que eles sejam de sua propriedade. A perspectiva de proteção de dados como um direito de propriedade, embora presente em alguns autores, não é a forma mais adequada de tratá-los. Os dados pessoais, segundo Laura Schertel Mendes, ‘podem se constituir em uma representação virtual da pessoa perante a sociedade’. Essa ligação entre os dados e a pessoa é tão forte que Stefano Rodota chega a falar em ‘corpo eletrônico’”.

O parágrafo terceiro do artigo 7º, inclusive, prevê que o “tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização” e o parágrafo sétimo trata do legítimo interesse para autorizar novos tratamentos nestes termos:

§7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei (BRASIL, 2018).

Muito embora seja um tema recente, já existe um posicionamento firmado no Superior Tribunal de Justiça sobre a responsabilização civil em caso de vazamento de dados.

O referido entendimento baseia-se na diferenciação de tutela a ser atribuída a um dado pessoal e a um dado pessoal sensível.

Neste sentido, entende o Superior Tribunal de Justiça:

PROCESSUAL CIVIL E ADMINISTRATIVO. INDENIZAÇÃO POR DANO MORAL. VAZAMENTO DE DADOS PESSOAIS. DADOS COMUNS E SENSÍVEIS. DANO MORAL PRESUMIDO. IMPOSSIBILIDADE. NECESSIDADE DE COMPROVAÇÃO DO DANO. I - Trata-se, na origem, de ação de indenização ajuizada por particular contra concessionária de energia elétrica pleiteando indenização por danos morais decorrentes do vazamento e acesso, por terceiros, de dados pessoais. II - A sentença julgou os pedidos improcedentes, tendo a Corte Estadual reformulada para condenar a concessionária ao pagamento da indenização, ao fundamento de que se trata de dados pessoais de pessoa idosa. III - A tese de culpa exclusiva de terceiro não foi, em nenhum momento, abordada pelo Tribunal Estadual, mesmo após a oposição de embargos de declaração apontando a suposta omissão. Nesse contexto, incide, na hipótese, a Súmula n. 211/STJ. In casu, não há falar em prequestionamento ficto, previsão do art. 1.025 do CPC/2015, isso porque, em conformidade com a jurisprudência do STJ, para sua incidência deve a parte ter alegado devidamente em suas razões recursais ofensa ao art. 1022 do CPC/2015, de modo a permitir sanar eventual omissão através de novo julgamento dos embargos de declaração, ou a análise da matéria tida por omissa diretamente por esta Corte. Tal não se verificou no presente feito. Precedente: AgInt no REsp 1737467/SC, Rel. Ministro Napoleão Nunes Maia Filho, Primeira Turma, julgado em 8/6/2020, DJe 17/6/2020. IV - O art. 5º, II, da LGPD, dispõe de forma expressa quais dados podem ser considerados sensíveis e, devido a essa condição, exigir tratamento diferenciado, previsto em artigos específicos. Os dados de natureza comum, pessoais mas não íntimos, passíveis apenas de identificação da pessoa natural não podem ser classificados como sensíveis. V - O vazamento de dados pessoais, a despeito de se tratar de falha indesejável no tratamento de dados de pessoa natural por pessoa jurídica, não tem o condão, por si só, de gerar dano moral indenizável. Ou seja, o dano moral não é presumido, sendo necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações. VI - Agravo conhecido e recurso especial parcialmente conhecido e, nessa parte, provido. (BRASIL. STJ - AREsp: 2.130.619 SP 2022/0152262-2, Data de

Julgamento: 07/03/2023, T2 - SEGUNDA TURMA, Data de Publicação: DJe 10/03/2023)

No referido caso, houve o compartilhamento indevido dos seguintes dados pessoais de uma consumidora pela concessionária de energia elétrica: nome completo, número do registro civil, gênero, data de nascimento, idade, números de telefone fixo e celular, endereço e dados relativos ao contrato para fornecimento de energia elétrica (carga instalada, consumo estimado, instalação e leitura).

Tais dados, em que pese sejam pessoais, ou seja, aptos a identificar a pessoa, não revelam nenhuma faceta da intimidade do indivíduo.

A sua divulgação não implica, em princípio, revelação de algo que o seu titular tivesse a opção de guardar unicamente para si.

O referido precedente revela o entendimento do STJ em relação à diferenciação de tutela entre os dados pessoais e os dados pessoais sensíveis.

Nesta linha, o acórdão destaca que os dados pessoais seriam dados comuns passíveis de identificação da pessoa natural, mas que estes não seriam íntimos, não podendo ser entendidos como sensíveis.

Neste sentido, no acórdão de relatoria do Ministro Francisco Falcão, foi destacado que o artigo 5º, inciso II, da LGPD traz um rol do que seriam os dados pessoais sensíveis e que demandariam, por sua vez, um tratamento diferenciado pelo sistema, nos termos do artigo 11 da LGPD.

No caso concreto, os dados vazados foram apenas dados pessoais, que podem ser fornecidos em qualquer cadastro, não estando protegidos por sigilo, sendo que o acesso por terceiros, em princípio, não atingiria o direito da personalidade, no entendimento do Superior Tribunal de Justiça.

Partindo desta diferenciação, foi firmado o entendimento pelo STJ de que o vazamento de dados pessoais, por si só, não gera dano moral indenizado<sup>32</sup>.

---

<sup>32</sup> Analisando o recente Precedente C-590 do Tribunal de Justiça da União Europeia, no que se refere ao entendimento daquele tribunal sobre a necessidade da prova de danos em situações de violação de dados pessoais, pontuou Faleiros Junior (2024, p. 1): “O precedente do TJUE no Processo C-590/22 é especialmente relevante,

Nesta linha, inexistindo presunção, deveria ter sido comprovada a existência de eventual dano, perante o caso concreto, no intuito de se conseguir uma indenização, o que não foi feito no caso analisado.

O acórdão destaca, ainda, que a situação seria diferente caso a ocorrência envolvesse o vazamento de dados sensíveis, por ter relação com a intimidade da pessoa natural, apontando que, nesta eventual hipótese, seria o caso de presumir-se a ocorrência de dano diante da natureza do bem protegido<sup>33</sup>.

Tal entendimento revela a atenção e o cuidado especial que deve ser dedicado aos dados pessoais sensíveis.

Ocorre, no entanto, que não se pode deixar de considerar que, com o cruzamento de dados, o vazamento aparentemente inofensivo de dados pode acarretar a obtenção de informações sensíveis, como já destacado.

---

pois clarifica que a mera violação do RGPD não é suficiente para garantir uma indenização, exigindo-se a demonstração do dano e seu nexo causal com a violação. Esta decisão orienta tanto os titulares dos dados quanto os responsáveis pelo tratamento na correta aplicação do RGPD, promovendo maior segurança jurídica e assegurando que os direitos individuais sejam efetivamente protegidos, enquanto se evitam pretensões infundadas. Como dito, o TJUE firmou o entendimento de que a mera violação do RGPD não é suficiente, por si só, para fundamentar um direito de indenização. Para que tal direito seja reconhecido, o titular dos dados deve demonstrar a existência de um dano causado pela violação. Essa interpretação reforça a necessidade de que haja nexo de causalidade entre a violação de preceitos do regulamento ou da legislação doméstica que o internalizou em cada país-membro da União Europeia e o dano sofrido, embora não seja necessário que o dano atinja um grau de reprovabilidade específico. Adicionalmente, o TJUE esclareceu que o receio de que dados pessoais tenham sido divulgados a terceiros, devido a uma violação do RGPD, pode ser suficiente para fundamentar um direito de indenização. No entanto, é imprescindível que esse receio, juntamente com suas consequências negativas, seja devidamente comprovado. Esse aspecto da decisão destaca a importância de considerar os efeitos psicológicos das violações de dados, que são de difícil mensuração”.

<sup>33</sup> Analisando de forma específica o referido acórdão, pontuou Faleiros Junior (2024, p. 2): “Apenas para fins de elucidação dos problemas interpretativos que ainda pairam no Brasil, em março de 2023, a Terceira Turma do STJ, no julgamento do AREsp 2.130.6196, de relatoria do Excelentíssimo ministro Francisco Falcão, adotou um posicionamento peculiar ao negar indenização por danos extrapatrimoniais pelo vazamento de dados comuns (não sensíveis) de uma cliente idosa, argumentando que o simples fato de vazamento desses dados não gera, por si só, um dano moral indenizável. O Tribunal enfatizou a necessidade de prova concreta do dano decorrente da exposição das informações, destacando que o risco de potencial fraude ou importunações não é suficiente para configurar dano moral “in re ipsa”. A decisão envolveu uma concessionária de serviço público (e, por isso, o precedente adveio da Terceira Turma), o que ensejou a aplicação da regra de responsabilização civil do Estado prevista no art. 37, § 6º, da Constituição da República. De todo modo, é importante frisar que não há, na LGPD, qualquer previsão que indique que, se dados pessoais sensíveis forem objeto de um “vazamento” se abrirá margem à admissão de dano moral “in re ipsa””.

Inclusive, o enunciado 690, aprovado na IX Jornada de Direito Civil do Conselho da Justiça Federal, prevê que: “A proteção ampliada conferida pela LGPD aos dados sensíveis deverá ser também aplicada aos casos em que houver tratamento sensível de dados pessoais, tal como observado no parágrafo primeiro do art. 11 da LGPD”.

Nesta linha, nos julgamentos referentes à responsabilidade civil decorrente de vazamento, esta questão deve ser sempre levada em consideração.

### **3. A PROTEÇÃO DE DADOS PESSOAIS NO PROCESSO JUDICIAL QUE NÃO TRAMITA EM SEGREDO DE JUSTIÇA**

#### **3.1 O ACESSO AOS AUTOS PROCESSUAIS E OS DADOS PESSOAIS CONSTANTES NA INICIAL**

A publicidade dos atos processuais, como já destacado em tópico antecedente, é uma garantia processual concedida às partes, assim como atende aos interesses de terceiros.

Com a publicização pretende-se garantir o direito à informação, desestimulando julgamentos escusos e possibilitando o controle dos atos judiciais<sup>34</sup>.

A inobservância desta garantia implica, inclusive, nulidade do ato processual, sendo que a Constituição Federal, em seus artigos 5º, inciso LX e 93, IX, admite a restrição à publicidade de atos processuais para defesa da intimidade ou quando o interesse social assim o exigir, prevendo a possibilidade de sigilo do processo, com a determinação do segredo de justiça.

Como já salientado, com o avanço da tecnologia, a questão da proteção dos dados pessoais nos processos judiciais é um tema que vem ganhando relevância, especialmente diante

---

<sup>34</sup> Neste sentido, pontua Roca (2020, p. 205): “La amplitud de la publicidad procesal puede ser respetuosa con la libertad de información del artículo 20 CE, pero a la vez cuestionar el contenido del derecho a la protección de datos. Um derecho que se construye sobre la idea del control de la información personal por parte del titular y que por lo tanto tiene difícil cohabitación con la publicidad procesal. Es ahora, em este momento en el que la preocupación por la protección de los datos personales cobra más relevância em el ámbito de la Administración de Justicia cuando nos planeamos como conviven ambos derechos fundamentales en el proceso y si procede la reducción de la publicidad para respetar el derecho a la protección de datos. No se trata tanto de elegir uno em detrimento del outro. Sino más bien buscar una interpretación de las normas a través del principio de proporcionalidade que permita conciliar la implementación de ambas garantías reduciendo em lo posible la colición indebida entre ambas. Tal y como já sido entendido este derecho fundamental, sancionado em el artículo 20 CE, presenta uma dimensión que transcende el próprio interés individual de los profesionales de la información, y se orienta aun fin coletivo "garanía de la posibilidad de existència de uma opinión pública libre, indisolublemente unida al pluralismo político próprio del Estado democrático”.

da vigência da LGPD no Brasil<sup>35</sup> e do reconhecimento dos direitos à proteção de dados e à autodeterminação informativa como fundamentais<sup>36</sup>.

Neste sentido, sobre a aplicabilidade dos princípios da proteção de dados no setor público, pondera Wimmer (2021, p. 283):

O art. 26 traz, ainda, outro elemento de grande relevância, que é o reconhecimento explícito de que os princípios de proteção de dados pessoais previstos na lei se aplicam ao compartilhamento de dados no setor público, atraindo, assim, a incidência de princípios, como o da finalidade, o da adequação, o da necessidade e o da não discriminação.

Em relação aos dados pessoais inseridos nos processos judiciais, cumpre destacar que a LGPD previu, em seus artigos 7º, inciso VI, § 3º e § 4º, assim como no 11º, inciso II, alínea “d”, que<sup>37</sup>:

---

<sup>35</sup> Sobre os esforços e empenho do Conselho Nacional de Justiça na adequação da atuação do Poder Judiciário à LGPD, pontua Santos (2021, p. 102): “O Poder Judiciário, assim como toda a Administração Pública brasileira, está enfrentando a complexidade e os desafios trazidos pela LGPD, pois ela demanda a (re)adequação de suas normas internas e de sua práxis, pois a legislação nacional infraconstitucional permite várias situações, as quais se abordarão a título exemplificativo, mais adiante. É importante referir que o Judiciário brasileiro está adequando-se à LGPD, via normatização expedida pelo Conselho Nacional de Justiça (CNJ), o qual, durante a sua 323ª sessão ordinária, em 15 de dezembro de 2020, aprovou uma resolução que padroniza os critérios dos tribunais brasileiros (com exceção do Supremo Tribunal Federal) para adequação à LGPD, indicando que cada tribunal deverá criar um Comitê Gestor de Proteção de Dados Pessoas (CGPD), órgão que será responsável pela implementação da lei, inclusive analisando o compartilhamento de dados em contratos e convênios”.

<sup>36</sup> Em análise realizada sobre o tratamento de dados pessoais na consulta de jurisprudência, entende o CNJ (2021, p. 6) que: “Dado o volume de dados pessoais tratados pelos tribunais brasileiros no exercício da função jurisdicional, impõe-se também ao Poder Judiciário o dever de conformar seus procedimentos ao novo ambiente normativo inaugurado pela LGPD. Nesse contexto, inspira especial cuidado a divulgação de decisões judiciais pelas páginas de pesquisa de jurisprudência mantidas pelos tribunais na internet. Os serviços de divulgação de jurisprudência devem estar permanentemente atentos à necessidade de equilíbrio entre publicidade processual e privacidade dos cidadãos e, diante dos novos elementos normativos introduzidos pela LGPD, não podem se furtar ao esforço de reavaliar o tratamento que conferem aos dados das pessoas naturais”.

<sup>37</sup> Sobre o tema, assinala Wimmer (2021, p. 279): “Com efeito, a natureza da relação entre cidadão e Poder Público, diferentemente da relação com atores privados, é compulsória e se configura como pré-condição para o exercício da cidadania. O tratamento de dados pessoais pelo Estado é imprescindível para o desempenho do seu mandato constitucional. A questão a ser enfrentada, portanto, é de assegurar que no desempenho de suas missões, inclusive na dimensão da normatização, a atuação do Poder Público se dê de maneira a buscar a concordância prática entre princípios como os da eficiência, do interesse público e da publicidade, e os princípios constantes da LGPD, como os da finalidade, da adequação e da necessidade, orientados pela ideia de autodeterminação informativa do cidadão. As diferenças na racionalidade de tratamento de dados entre setor público e iniciativa privada não foram desconsideradas na LGPD, que estabeleceu as bases legais próprias para o tratamento de dados pelo Poder Público e um capítulo específico para o tema, declarando, logo no primeiro artigo do capítulo, que tal tratamento deve ter por objetivo 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. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

[...]

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

[...]

§ 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.

§ 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.

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

[...]

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem). (BRASIL, 2018).

Em especial, o art. 7º da LGPD prevê que o tratamento de dados pessoais de acesso público deve ser realizado com base na finalidade, boa-fé e interesse público, que amparam a sua divulgação, sendo possível a realização de novos tratamentos desde que atendidos propósitos legítimos para isto, respeitando o direito do titular, assim como os fundamentos da lei.

Neste particular, pondera Wimmer (2021, p. 280):

O deslinde dessa questão se dá pela leitura do art. 23 da LGPD, que estabelece uma hipótese complementar para o tratamento de dados pelo Poder Público, ao acrescentar às previsões dos arts. 7º e 11 o objetivo de “executar as competências legais ou cumprir as atribuições legais do serviço público”. Compreende-se, assim, que, no que tange às bases legais específicas para o tratamento de dados pessoais pelo Poder Público, a LGPD prevê duas hipóteses centrais: (i) execução de políticas públicas; e (ii) execução de competências legais ou atribuições legais do serviço público.

[...].

Assim, entende-se que, em harmonia com o próprio princípio da legalidade, que limita a atuação do Estado àquelas competências que lhe são atribuídas pela lei, o tratamento de dados pessoais pelo Poder Público deve, em regra, se dar ao abrigo de suas competências legais, ficando as demais hipóteses legais relegadas à condição de exceções.

No que tange a questão do consentimento para tratamento de dados em processos judiciais, nestes casos, pontua Cueva (2020, p. 206):

Para tanto, a primeira questão a examinar diz respeito ao consentimento, a pedra angular dos sistemas de tutela de dados pessoais. Pressupõe-se que quem postule ou atue de algum modo perante o Poder Judiciário tenha dado seu consentimento para que seus dados sejam processados, a fim de tornar possível a prestação jurisdicional que de outro modo não poderia ser dispensada, pois a atividade típica do judiciário deve ser exercida sob um grau maior ou menor de publicidade, dependendo do contexto e da legislação aplicável. O problema reside, então, em saber se a finalidade para a qual todos os dados foram coletados, armazenados e processados foi ou não desviada.

No Brasil, a LGPD é parcimoniosa nas referências à atividade jurisdicional, mas autoriza expressamente o tratamento de dados, inclusive de dados sensíveis, para o exercício regular de direitos em processo judicial, administrativo e arbitral (art. 7º, VI, e 11, II, d, da LGPD).

Já no que se refere ao atendimento à finalidade pretendida, à boa-fé e ao acesso público, adverte Cueva (2020, p. 202):

É obrigatória a observância dos princípios da finalidade, da boa-fé e do interesse público no tratamento de dados pessoais cujo acesso é público, uma vez que o titular de dados, ainda que os torne manifestamente públicos, preserva seus direitos (Par. 3º e 4º do art 7º da LGPD).

A Lei n. 13.793, de 2019, e a Resolução 121/2010, em nome da transparência, proporcionam o amplo acesso a íntegra dos processos, que dispõem de dados pessoais e – muitas vezes – dados sensíveis das partes envolvidas.

Neste sentido, esclarece Cueva (2020, p. 201):

Paralelamente ao aprimoramento da legislação de proteção da privacidade, cresce a demanda social por maior transparência da atuação do Estado. Surgem em vários países, já no limiar do século XXI, as leis destinadas a garantir amplo acesso à informação acerca das atividades do Estado. No Brasil, a Lei de Acesso à Informação (Lei n. 12.527/2011, ou LAI) procura assegurar a qualquer cidadão amplo acesso a informações e dados públicos.

Neste cenário de grande avanço tecnológico e de ampla disponibilização de dados: pessoais nos processos, Cueva (2020, p. 205) ainda pondera:

Não há dúvidas de que os advogados já dispunham de amplo direito de acesso à integralidade dos autos, assegurado pelo Estatuto dos Advogados e da OAB (art. 7º, XIII) e pelo CPC (art. 107, I). Porém, a trivialização e o barateamento das tecnologias de acesso, processamento e divulgação de informações, em situação muito discrepante daquela na qual o acesso aos autos certáceos somente ocorria nas secretarias judiciais, levam a indagar se não há colisão entre valores fundamentais, a publicidade e a transparência, de um lado, e a proteção da intimidade e da vida privada, de outro.

A existência, na atualidade, de *softwares* e sistemas de inteligência artificial aptos a obter e processar dados encontrados em processos judiciais, no intuito de utilizá-los, inclusive comercialmente, o que não ocorria quando os processos eram físicos, justifica uma atenção especial em relação ao tema.

Diante da vulnerabilidade das informações pessoais contidos nos bancos de dados dos tribunais, tem sido frequente o relato de casos de realização de novos tratamentos para finalidades distintas daquelas que justificaram sua inserção nos processos.

Caso os dados sejam disponibilizados e coletados, não é possível controlar os tratamentos passíveis de ocorrer, o que compromete a autodeterminação informativa.

O banco de dados do Poder Judiciário, neste cenário, pode se tornar uma verdadeira fonte de informações para a violação dos direitos da personalidade dos indivíduos.

Sobre o enriquecimento e a utilização indevida de dados pessoais, Mendes e Fonseca (2021, p. 82-83) pontuam:

Dados considerados “irrelevantes” ou “públicos” como idade, altura, nacionalidade, os locais de moradia e de trabalho podem servir de insumos pra correlações, predições e ranqueamentos acerca da personalidade do titular dos dados pessoais ou de determinados grupos sociais. Essas decisões têm a capacidade prática de determinar “a vida das pessoas: desde a seleção de currículos para uma vaga de emprego, chegando até os seguros, acesso ao crédito e serviços de governo. Em suma, a criação de detalhados perfis a respeito dos cidadãos pode criar sérios riscos à sua personalidade na medida em que essas representações virtuais têm o condão de diminuir ou de aumentar oportunidades sociais “em aspectos centrais da vida humana”, como “emprego, moradia, crédito, justiça criminal, justamente de acordo com a classificação ou o *score* conferido ao seu perfil. Dessa maneira, dados inexatos ou incompletos e vieses do programador do algoritmo, por exemplo, podem gerar predições, interferências e interpretações verdadeiramente discriminatórias acerca de um indivíduo ou de um segmento social.

Os referidos programas, via de regra, conseguem “enriquecer” os dados obtidos por meio dos processos judiciais mediante o cruzamento de bases existentes, criando informações consolidadas que poderão ser utilizadas para diversas outras finalidades<sup>38</sup>.

---

<sup>38</sup> Neste particular, Doneda e Machado (2021, p. 344) esclarecem que: “Pode-se dizer o mesmo de situações de agregação, mineração e tratamento de dados combinados, casos em que se permite a descoberta, com base em dados simples, de outras situações sensíveis. Tal possibilidade permite a criação de uma “biografia digital” das pessoas. Muitas vezes, pedaços de informação, que parecem inofensivos, podem ser o “link que falta” de um “detalhe crítico”, ou ainda “a chave necessária para destrancar outras lojas de informações pessoais.”

Este estudo entende que os dados pessoais contidos em um processo podem ser classificados em: (i) dados pessoais não relacionados à causa de pedir; (ii) dados pessoais relacionados à causa de pedir; e (iii) dados pessoais sensíveis e íntimos.

Os dados pessoais não relacionados à causa de pedir são dados pessoais que não têm interesse ao conflito em si. Uma petição inicial, por exemplo, é repleta de dados pessoais relacionados à qualificação das partes, o que inclui o nome, a nacionalidade, o estado civil, a profissão, o domicílio, os números de documentos pessoais (como registro civil, cadastro de pessoa física, carteira de trabalho, dentre outros), a linha telefônica móvel celular e o endereço de e-mail – nos termos da Resolução 345 de 2020 do Conselho Nacional de Justiça para adesão ao Juízo 100% Digital - e, em alguns casos, os nomes dos seus genitores; assim como informações sobre condições pessoais<sup>39</sup>.

Estes dados visam, exclusivamente, a precisa identificação perante o Juízo e a outra parte, ou seja, é de interesse no âmbito endoprocessual, motivo pelo qual inexistiria interesse público em seu acesso - o que será considerado na proposta de restrição de acesso formulada no tópico final desta tese.

Em relação ao nome, no entanto, entendemos que a divulgação do referido dado atende ao interesse público, especialmente, no que se refere à identificação e ao controle referente a casos de litispendência, conexão, continência e coisa julgada.

Ressalvadas as hipóteses de homonímia, com o nome da parte, na maioria dos casos, é possível identificar a ocorrência destas situações, o que justificaria a sua divulgação.

É certo que alguns dos dados listados acima poderão estar vinculados à causa de pedir a depender do caso concreto.

---

<sup>39</sup> No relatório da análise realizada sobre o tratamento de dados pessoais na consulta de jurisprudência, pontuou o CNJ (2021, p. 8) que: “Ocorre, todavia, que, no atual estágio de desenvolvimento tecnológico, já não é mais possível afirmar candidamente a irrestrita publicidade de informações judiciais sem levar em consideração os riscos concretos que ela pode oferecer à privacidade dos cidadãos. Os processos judiciais são uma fonte inesgotável de dados pessoais (inclusive sensíveis) titularizados pelos mais variados atores processuais (partes, testemunhas, vítimas, magistrados(as), advogados(as), auxiliares da justiça etc.) e por 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”.

Já os dados pessoais relacionados à causa de pedir são aqueles que têm relação com o conflito e que, por este motivo, devem ser necessariamente publicizados, para que sejam compreendidos os limites objetivos da lide.

Por sua vez, os dados sensíveis e os dados íntimos, embora possam ter ou não relação com a causa de pedir, merecem uma atenção diferenciada.

Conforme destacado em tópico anterior, os dados pessoais sensíveis são aqueles que “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, quando vinculado a uma pessoa natural”.

Os íntimos são aqueles que, pela sua natureza, são guardados pelo seu titular e faz referência a algo de sua essência.

Pela sua essência, estes dados merecem estar sob sigilo, em atenção ao livre desenvolvimento da personalidade, o que será considerado na proposta a ser formulada.

Diante da realidade atual, nos processos que não tramitam em segredo de justiça, todos os dados estão acessíveis e podem vir a ser objeto de tratamento através de recursos tecnológicos, que traduzem a pessoa em algoritmos.

Sobre esta realidade, Rosenvald (2021) assevera que:

Nesta inédita forma de mercado a pessoa se atomiza no indivíduo, mero conjunto de algoritmos passíveis de comercialização. Infere-se que a noção de expropriação da personalidade rompe com um dos muros de contenção das situações existenciais, pois a renderização da experiência humana não equivale a uma simples cessão temporária do exercício econômico de nossa imagem, intimidade ou nome, porém do próprio confisco do conteúdo daquilo que nos singulariza, para posterior operação lucrativa no insaciável mercado de comportamento futuro. Em síntese, ao contrário da previsão do art. 11 do Código Civil, os direitos da personalidade se tornam "absolutamente disponíveis" e suscetíveis de limitação heterônoma.

Desse modo, mostra-se necessária a criação de um modelo para limitar o amplo acesso a informações pessoais nos processos.

### 3.2 O CRUZAMENTO DE DADOS: A DIVULGAÇÃO POR PROVEDOR DE APLICAÇÕES DE INTERNET DE CONTEÚDOS DE PROCESSOS JUDICIAIS - O TEMA 1141 DO SUPREMO TRIBUNAL FEDERAL

Evidenciados os riscos do tratamento indevido de informações constantes em processos judiciais no tópico anterior, este estudo passa a analisar o Agravo em Recurso Extraordinário de n. 1307386, que foi destacado como *Leading case* para discutir o tema “Responsabilidade civil por disponibilização na internet de informações processuais publicadas nos órgãos oficiais do Poder Judiciário, sem restrição de segredo de justiça ou obrigação jurídica de remoção”, que configura o tema 1141 do Supremo Tribunal Federal.

No referido tema, discute-se, à luz dos artigos 5º, II, IX, XIV, XXXIII, XXXVI e LX, 37, 93, IX e 220 da Constituição Federal, a licitude ou não da divulgação por “provedor de aplicações de internet de conteúdos de processos judiciais, em andamento ou findos, que não tramitem em segredo de justiça, e nem exista obrigação jurídica de removê-los, de modo a ampliar a abrangência territorial de tese firmada por tribunal estadual em incidente de resolução de demandas repetitivas - IRDR”.

A ação destacada foi originalmente movida contra as empresas “ESCAVADOR” e “GOOGLE DO BRASIL”, perante o Juízo da 5ª Vara Cível da Comarca de Pelotas-RS e registrada sob o número 0002923-15.2016.8.21.0022, tendo natureza indenizatória em virtude de supostos danos morais sofridos.

Para a exata compreensão do que está sendo discutido no tema 1141, cumpre destacar que, na inicial da referida ação, o autor sustenta que teria digitado o seu nome no site de buscas *Google* e que teria surgido como resultado uma referência no site Escavador, que estaria divulgando informações pessoais suas sobre a reclamação trabalhista em que ele era parte, o que lhe teria causado prejuízos e violado a Resolução 139/14 do Conselho Superior da Justiça do Trabalho (CSJT).

A Resolução 139, de 2014, como destacado no tópico 1.2 deste estudo, determina que os Tribunais Regionais do Trabalho incorporem meios para coibir o acesso automatizado a dados dos reclamantes contidos em reclamações trabalhistas para impedir a criação das

conhecidas “listas sujas”<sup>40</sup>, em que constam os trabalhadores que moveram reclamações trabalhistas contra seus empregadores. A resolução determina, ainda, que sejam adotadas ações para impedir indexações dos sites de busca por meio do desenvolvimento de soluções tecnológicas.

Diante da violação da referida resolução, o autor busca, por meio da mencionada ação, a exclusão imediata e definitiva de toda e qualquer informação a seu respeito, pessoal e profissional, da internet, bem como a indenização por danos morais.

Em sua defesa, a empresa Google suscitou - além de questões processuais relacionadas à suposta ausência no interesse de agir -, que seria entendimento consolidado nos tribunais nacionais de que a ferramenta de pesquisas não pode remover determinados *links*, a ineficácia da medida em razão da remoção não impedir que o conteúdo seja localizado no site de origem<sup>41</sup>, a inexistência de ato ilícito, assim como a ausência de danos morais sofridos.

---

<sup>40</sup> Neste particular, Oliveira e Silva (2023, p. 11) ponderam que: “É importante que se diga que, diante da ausência de disposição legal específica ou de regulamentação do CNJ, no contexto legislativo atual, são formulados diversos pedidos, para que os processos tramitem em segredo de justiça ou para que os dados pessoais sejam anonimizados, sob o fundamento de um possível prejuízo em futuras contratações por meio das “listas sujas de trabalhadores”, havendo decisões divergentes sobre tal questão. Algumas acolhem o pedido de supressão dos nomes das partes, com base na LGPD (Processo: 1000902-06.2019.5.02.0707 e outras), enquanto outras entendem que a proteção conferida pelas regras vigentes já seria suficiente, indeferindo tal pleito (Processo: 1001089-83.2020.5.02.0317 e outros). Assim, para garantia da privacidade das partes e testemunhas, com a preservação da autodeterminação informativa e garantia do direito fundamental à proteção de dados, faz-se necessária a adoção de meios para a anonimização dos registros tornados públicos pela política de open justice adotada pelo CNJ. Nem se diga que a adoção de tal medida inviabilizaria a atuação das lawtechs, pois, conforme destacado no supracitado relatório da Lawgorithm, a atuação das referidas empresas concentram-se mais nos pronunciamentos judiciais, nas petições e, em menor medida nos documentos pessoais das partes, sem a exploração dos aspectos pessoais das partes. Tal constatação demonstra que eventual medida de anonimização dos dados identificadores de pessoas físicas envolvidas nos processos teria pouco impacto nas atividades de tecnologia aplicada aos dados judiciais, sendo fundamental para a proteção da privacidade dos envolvidos”.

<sup>41</sup> Sobre a ausência de responsabilidade dos provedores de aplicação por documentos produzidos por terceiros, entendeu o Superior Tribunal de Justiça, em incidente de uniformização de jurisprudência, que: “CIVIL, PROCESSO CIVIL E CONSUMIDOR. RECLAMAÇÃO. RESOLUÇÃO 12/09 DO STJ. DECISÃO TERATOLÓGICA. CABIMENTO. INTERNET. PROVEDOR DE PESQUISA VIRTUAL. FILTRAGEM PRÉVIA DAS BUSCAS. DESNECESSIDADE. RESTRIÇÃO DOS RESULTADOS. NÃO-CABIMENTO. CONTEÚDO PÚBLICO. DIREITO À INFORMAÇÃO. DADOS OFENSIVOS ARMAZENADOS EM CACHE. EXCEÇÃO. EXCLUSÃO. DEVER, DESDE QUE FORNECIDO O URL DA PÁGINA ORIGINAL E COMPROVADA A REMOÇÃO DESTA DA INTERNET. COMANDO JUDICIAL ESPECÍFICO. NECESSIDADE. ASTREINTES. OBRIGAÇÃO IMPOSSÍVEL. DESCABIMENTO. DISPOSITIVOS LEGAIS ANALISADOS: ARTS. 220, § 1º, da CF/88, 461, § 5º, do CPC. 1. Embora as reclamações ajuizadas com base na Resolução nº 12/2009 do STJ a rigor somente sejam admissíveis se demonstrada afronta à jurisprudência desta Corte, consolidada em enunciado sumular ou julgamento realizado na forma do art. 543-C do CPC, afigura-se possível, excepcionalmente, o conhecimento de reclamação quando ficar evidenciada a teratologia da decisão reclamada. 2. A filtragem do conteúdo das pesquisas feitas por cada usuário não constitui atividade intrínseca ao serviço prestado pelos provedores de pesquisa virtual, de modo que não se pode reputar defeituoso o site que não exerce esse controle sobre os resultados das buscas. 3. Os provedores de pesquisa virtual realizam suas buscas dentro de um universo virtual, cujo acesso é público e irrestrito, ou seja, seu papel se restringe à identificação de páginas na web onde determinado dado ou informação, ainda que ilícito, estão sendo livremente veiculados. Dessa forma, ainda que seus mecanismos de busca facilitem o acesso e a consequente divulgação de páginas cujo

Neste particular, vale destacar que existem decisões proferidas pelo Superior Tribunal de Justiça sobre o referido assunto, em especial, aquela proferida no Recurso Especial de n. 1.316.921/RJ, de relatoria da Ministra Nancy Andrighi, em ação movida pela apresentadora Maria da Graça Xuxa Meneghel, que buscou a exclusão de suas imagens do resultado do mencionado site de buscas, o que também foi sustentado pela Google.<sup>42</sup>

A Google sustentou também que os provedores de pesquisa buscariam informações dentro de um universo digital, que é de acesso público, sendo que o livre acesso à informação sobre os processos não feriria este direito, nos termos do art. 220 da CF.<sup>43</sup>

---

conteúdo seja potencialmente ilegal, fato é que essas páginas são públicas e compõem a rede mundial de computadores e, por isso, aparecem no resultado dos sites de pesquisa. 4. Os provedores de pesquisa virtual não podem ser obrigados a eliminar do seu sistema os resultados derivados da busca de determinado termo ou expressão, tampouco os resultados que apontem para uma foto ou texto específico, independentemente da indicação do URL da página onde este estiver inserido. 5. Não se pode, sob o pretexto de dificultar a propagação de conteúdo ilícito ou ofensivo na web, reprimir o direito da coletividade à informação. Sopesados os direitos envolvidos e o risco potencial de violação de cada um deles, o fiel da balança deve pender para a garantia da liberdade de informação assegurada pelo art. 220, § 1º, da CF/88, sobretudo considerando que a Internet representa, hoje, importante veículo de comunicação social de massa. 6. Preenchidos os requisitos indispensáveis à exclusão, da web, de uma determinada página virtual, sob a alegação de veicular conteúdo ilícito ou ofensivo - notadamente a identificação do URL dessa página - a vítima carecerá de interesse de agir contra o provedor de pesquisa, por absoluta falta de utilidade da jurisdição. Se a vítima identificou, via URL, o autor do ato ilícito, não tem motivo para demandar contra aquele que apenas facilita o acesso a esse ato que, até então, se encontra publicamente disponível na rede para divulgação. 7. Excepciona o entendimento contido nos itens anteriores o armazenamento de dados em cache. Estando uma cópia do texto ou imagem ofensivos ou ilícitos registrados na memória cache do provedor de pesquisa virtual, deve esse, uma vez ciente do fato, providenciar a exclusão preventiva, desde que seja fornecido o URL da página original, bem como comprovado que esta já foi removida da Internet. 8. Como se trata de providência específica, a ser adotada por pessoa distinta daquela que posta o conteúdo ofensivo e envolvendo arquivo (cópia) que não se confunde com o texto ou imagem original, deve haver não apenas um pedido individualizado da parte, mas um comando judicial determinado e expresso no sentido de que a cópia em cache seja removida. 9. Mostra-se teratológica a imposição de multa cominatória para obrigação de fazer que se afigura impossível de ser cumprida. 10. Reclamação provida”. (BRASIL. Superior Tribunal de Justiça. Rcl: 5072 AC 2010/0218306-6, Relator: Ministro MARCO BUZZI, Data de Julgamento: 11/12/2013, S2 - SEGUNDA SEÇÃO, Data de Publicação: DJe 04/06/2014).

<sup>42</sup> No Recurso Especial de n. 1.316.921/RJ, foi entendido que: “[...]. 7. Não se pode, sob o pretexto de dificultar a propagação de conteúdo ilícito ou ofensivo na web, reprimir o direito da coletividade à informação. Sopesados os direitos envolvidos e o risco potencial de violação de cada um deles, o fiel da balança deve pender para a garantia da liberdade de informação assegurada pelo art. 220, parágrafo primeiro, da CF/88, sobretudo considerando que a internet representa, hoje, importante veículo de comunicação de massa. 8. Preenchidos os requisitos indispensáveis à exclusão, da web, de uma determinada página virtual, sob a alegação de veicular conteúdo ilícito ou ofensivo – notadamente a identificação do URL dessa página – a vítima carecerá de interesse de agir contra o provedor de pesquisa, por absoluta falta de utilidade de jurisdição. Se a vítima identificou, via URL, o autor do ato ilícito, não tem motivo para demandar contra aquele que apenas facilita o acesso a esse ato que, até então, se encontra publicamente disponível na rede para divulgação”.

<sup>43</sup> Prevê o art. 220 da Constituição Federal que “Art. 220. A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição”.



A sentença proferida no mencionado processo entendeu que não existia responsabilidade a ser imputada a empresa Google, pois a mesma oferece apenas uma ferramenta de busca de informações disponibilizadas por terceiros e que esta não tem ingerência sobre os conteúdos veiculados pelos sites. Também foi destacado que, nos termos do parágrafo 1º, do art. 19, da Lei 12.965 de 2014, o “Marco Civil da Internet”<sup>44</sup>, o Google somente responderia no caso de descumprimento de ordem judicial.

Ademais, a sentença ainda julgou improcedente a ação contra a ré Escavador – que sequer apresentou defesa -, por entender que não houve ilícito imputável a referida empresa, pois esta só teria disponibilizado pesquisa de internet, realizada por meio dos sites dos tribunais.

No recurso interposto pela parte autora, foi sustentado que o Escavador usa técnicas de mineração de dados, por meio das quais informações de difícil compreensão são convertidas em informações úteis.

Nas contrarrazões apresentadas pelo site “Escavador”, foi destacado que suas atividades consistiriam em coletar dados públicos e disponibilizá-los, após organização prévia. Os textos dos diários oficiais seriam diariamente capturados e, em seguida, aplicados algoritmos de inteligência artificial<sup>45</sup> para sistematizar os dados. Foi apontado ainda que, inicialmente, os dados eram coletados apenas da Plataforma *Lattes*, mas, após expansão e desenvolvimento do robô de busca, informações dos Diários Oficiais e do Instituto Nacional de Propriedade Industrial também passaram a ser contempladas.

Ademais, a empresa afirma que o sistema não disponibilizava informações sobre o andamento processual, informações pessoais e arquivos em formato *pdf*, não interagindo com

---

<sup>44</sup> Dispõe o referido artigo que: “Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário. § 1º A ordem judicial de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material [...]”.

<sup>45</sup> Neste particular, Oliveira e Silva (2023, p. 8) ponderam que: “A partir do desenvolvimento de mecanismos de inteligência artificial, os dados judiciais passaram a ser utilizados para a identificação de diversas informações importantes que, a depender do contexto de uso, irão permitir a identificação de padrões estatísticos (jurimetria) ou a análise preditiva de julgados. Tal prática decorre de uma técnica desenvolvida a partir da década de 80, conhecida como mineração de dados (garimpagem, profiling ou datamining), que consiste essencialmente em extrair informação de gigantescas bases de dados da maneira mais automatizada possível”.

os *sites* dos tribunais. Além disso, permite que qualquer usuário requeira a exclusão das informações obtidas pela plataforma.

Houve ainda a instauração do Incidente de Resolução de Demandas Repetitivas (IRDR) de n. 0233575-44.2019.8.21.7000, sendo a causa-piloto a referida demanda analisada por este estudo, em razão de inúmeras decisões contraditórias e a inexistência, naquele momento, de recurso afetado para definição de tese em tribunais superior.

A empresa buscava a fixação de tese, por meio do IRDR, de que seria “lícita a divulgação, por provedor de aplicações de internet, de conteúdos de processos judiciais (em andamento ou findos) que não tramitem em segredo de justiça, e, conseqüentemente, não existe obrigação jurídica de removê-los”<sup>46</sup>.

Outro argumento utilizado na demanda é que a liberdade de informação, prevista no inciso IX do artigo 5º e no art. 220 da CF, também compreende o direito de informar, de ser informado e de se informar, que deve ser conformado com o direito ao esquecimento<sup>47</sup>, que não tem previsão legal.

---

<sup>46</sup> Vale destacar que, no procedimento de PEDIDO DE PROVIDÊNCIAS, n. 0003869-39.2016.2.00.0000, o Conselho Nacional de Justiça assim decidiu: “RECURSO ADMINISTRATIVO EM PEDIDO DE PROVIDÊNCIAS. FORMAÇÃO DE “LISTAS NEGRAS”. PROCESSOS SUJEITOS À APRECIÇÃO DA JUSTIÇA DO TRABALHO. PRÁTICA DISCRIMINATÓRIA EM FACE DE EMPREGADOS QUE RECORREM AO PODER JUDICIÁRIO PARA O RECEBIMENTO DE VERBAS TRABALHISTAS. RESOLUÇÕES CNJ N. 121 E 143. SISTEMA PJE. RESTRIÇÃO DE INFORMAÇÕES EM CONSULTAS PÚBLICAS NOS SISTEMAS DE TRAMITAÇÃO E ACOMPANHAMENTO PROCESSUAL DOS TRIBUNAIS E CONSELHOS. PUBLICAÇÃO DOS NOMES DAS PARTES E DE SEUS ADVOGADOS NOS DIÁRIOS ELETRÔNICOS DOS TRIBUNAIS. NECESSÁRIA ALTERAÇÃO LEGISLATIVA. PRETENSÃO DE TRATAMENTO DE EXCEÇÃO AO PROCESSO TRABALHISTA. SEGREDO DE JUSTIÇA. IMPOSSIBILIDADE. PRINCÍPIO DA PUBLICIDADE DOS ATOS PROCESSUAIS. RECURSO DESPROVIDO. I. O Sistema PJe observa integralmente o regramento da Resolução CNJ n. 121, com as alterações inseridas pela Resolução CNJ n. 143, restringindo as consultas públicas dos sistemas de tramitação e acompanhamento processual dos Tribunais e Conselhos, nos processos sujeitos à apreciação da Justiça do Trabalho, ao número atual ou anteriores, inclusive em outro juízo ou instâncias, nomes dos advogados e registro na Ordem dos Advogados do Brasil. II. A efetiva proteção dos dados de demandantes na Justiça do Trabalho depende de alteração legislativa que afaste a obrigatoriedade de publicação dos nomes das partes, contida no art. 272, § 2º, do Código de Processo Civil. III. Não se pode determinar que toda e qualquer ação trabalhista tramite em segredo de justiça, seja em razão do princípio da publicidade dos atos processuais, que inviabiliza que se trate como regra o que é medida excepcional, seja pela incompetência deste Órgão para tal determinação, uma vez que a decisão é tomada individualmente no bojo do processo judicial. IV. Na propositura da ação, a própria parte pode requerer segredo de justiça para os autos processuais ou sigilo para um ou mais documentos ou arquivos do processo. V. Ausência nas razões recursais, de argumentos capazes de abalar os fundamentos da Decisão combatida. Recurso conhecido e desprovido”.

<sup>47</sup> Com fundamento no direito ao esquecimento, dentre outros, o Superior Tribunal de Justiça já decidiu no sentido de determinar que os provedores de pesquisa restrinjam acesso a resultados em nome da intimidade, proteção de dados, dados pessoais e direito ao esquecimento, como referido no aludido processo: “RECURSO ESPECIAL. DIREITO CIVIL. AÇÃO DE OBRIGAÇÃO DE FAZER. 1. OMISSÃO, CONTRADIÇÃO OU OBSCURIDADE. AUSÊNCIA. 2. JULGAMENTO EXTRA PETITA. NÃO CONFIGURADO. 3. PROVEDOR

O Incidente de Resolução de Demandas Repetitivas foi acolhido, tendo sido desprovido o recurso no processo-piloto e fixada tese jurídica, nos seguintes termos:

APELAÇÃO CÍVEL/CAUSA-PILOTO. INCIDENTE DE RESOLUÇÃO DE DEMANDA REPETITIVA - IRDR. RESPONSABILIDADE CIVIL. DISPONIBILIZAÇÃO DE INFORMAÇÕES PROCESSUAIS NA INTERNET PUBLICADAS PELO PODER JUDICIÁRIO SEM RESTRIÇÃO DE SEGREDO DE JUSTIÇA. INOCORRÊNCIA DE ATO ILÍCITO. FIXAÇÃO DE TESE. 1. Trata-se de julgamento conjunto de incidente de resolução de demandas repetitivas - IRDR (70082616665) oriundo de apelação cível interposta nos autos do processo nº 022/1.16.0001333-1, com objetivo de fixação da tese jurídica aplicável, na forma do art. 987, caput, do CPC, bem como do julgamento da causa-piloto nos termos do art. 987, parágrafo único, do diploma processual cível precitado. 2. A Constituição Federal consagra em seu art. 5º, inciso LX, o caráter público do processo como regra geral, sendo permitida a restrição da publicidade apenas nos casos em que a defesa da intimidade ou o interesse social o exigir. 3. A Resolução 121/2010 do Conselho Nacional de Justiça – CNJ, ao tratar divulgação de dados processuais eletrônicos na rede mundial de computadores, estabelece o livre acesso a diversos dados processuais, inclusive o inteiro teor das decisões, sentenças, votos e acórdãos. 4. Na Resolução precitada, simplesmente há a restrição quanto à consulta pelo nome das partes no sistema informatizado da Justiça do Trabalho. Já nos processos criminais, nos casos especificados no inciso I do §1º acima mencionado, a consulta deve ser somente pelo número do processo. No entanto, não resta inviabilizada a coleta desses dados mediante a publicação constante no Diário Oficial em nenhum dos casos. 5. Portanto, é lícita a consulta de dados judiciais quanto às ações intentadas, excetuando o nome atinente aos processos submetidos a segredo de justiça, hipótese na qual, via de regra,

---

DE APLICAÇÃO DE PESQUISA NA INTERNET. PROTEÇÃO A DADOS PESSOAIS. POSSIBILIDADE JURÍDICA DO PEDIDO. DESVINCULAÇÃO ENTRE NOME E RESULTADO DE PESQUISA. PECULIARIDADES FÁTICAS. CONCILIAÇÃO ENTRE O DIREITO INDIVIDUAL E O DIREITO COLETIVO À INFORMAÇÃO. 4. MULTA DIÁRIA APLICADA. VALOR INICIAL EXORBITANTE. REVISÃO EXCEPCIONAL. 5. RECURSO ESPECIAL PARCIALMENTE PROVIDO. 1. Debate-se a possibilidade de se determinar o rompimento do vínculo estabelecido por provedores de aplicação de busca na internet entre o nome do prejudicado, utilizado como critério exclusivo de busca, e a notícia apontada nos resultados. 2. O Tribunal de origem enfrentou todas as questões postas pelas partes, decidindo nos estritos limites da demanda e declinando, de forma expressa e coerente, todos os fundamentos que formaram o livre convencimento do Juízo. 3. A jurisprudência desta Corte Superior tem entendimento reiterado no sentido de afastar a responsabilidade de buscadores da internet pelos resultados de busca apresentados, reconhecendo a impossibilidade de lhe atribuir a função de censor e impondo ao prejudicado o direcionamento de sua pretensão contra os provedores de conteúdo, responsáveis pela disponibilização do conteúdo indevido na internet. Precedentes. 4. Há, todavia, circunstâncias excepcionalíssimas em que é necessária a intervenção pontual do Poder Judiciário para fazer cessar o vínculo criado, nos bancos de dados dos provedores de busca, entre dados pessoais e resultados da busca, que não guardam relevância para interesse público à informação, seja pelo conteúdo eminentemente privado, seja pelo decurso do tempo. 5. Nessas situações excepcionais, o direito à intimidade e ao esquecimento, bem como a proteção aos dados pessoais deverá preponderar, a fim de permitir que as pessoas envolvidas sigam suas vidas com razoável anonimato, não sendo o fato desabonador corriqueiramente rememorado e perenizado por sistemas automatizados de busca. 6. O rompimento do referido vínculo sem a exclusão da notícia compatibiliza também os interesses individual do titular dos dados pessoais e coletivo de acesso à informação, na medida em que viabiliza a localização das notícias àqueles que direcionem sua pesquisa fornecendo argumentos de pesquisa relacionados ao fato noticiado, mas não àqueles que buscam exclusivamente pelos dados pessoais do indivíduo protegido. 7. No caso concreto, passado mais de uma década desde o fato noticiado, ao se informar como critério de busca exclusivo o nome da parte recorrente, o primeiro resultado apresentado permanecia apontando link de notícia de seu possível envolvimento em fato desabonador, não comprovado, a despeito da existência de outras tantas informações posteriores a seu respeito disponíveis na rede mundial. 8. O arbitramento de multa diária deve ser revisto sempre que seu valor inicial configure manifesta desproporção, por ser irrisório ou excessivo, como é o caso dos autos. 9. Recursos especiais parcialmente providos”. (BRASIL. REsp 1660168/RJ. Rel. Ministra NANCY ANDRIGHI, Rel. p/ Acórdão Ministro MARCO AURÉLIO BELLIZZE, TERCEIRA TURMA, julgado em 08/05/2018, DJe 05/06/2018).

a ação trabalhista não se enquadra, não havendo, portanto, óbice à divulgação das informações referentes aos processos trabalhistas ou até mesmo criminais. 6. Assim, cumpre destacar a licitude da atividade exercida pela proponente, a qual apenas reproduz as informações disponibilizadas pelo Diário Eletrônico da Justiça, sendo, portanto, hipótese de exercício regular de direito, não havendo que se falar na prática de ato que ateste direito de indenização. 7. Fixação da seguinte tese jurídica: É lícita a divulgação por provedor de aplicações de internet de conteúdos de processos judiciais, em andamento ou findos, que não tramitem em segredo de justiça, e nem exista obrigação jurídica de removê-los da rede mundial de computadores, bem como a atividade realizada por provedor de buscas que remeta aquele. 8. Assim, fixada a tese jurídica quanto ao tema tratado na causa-piloto, o resultado desta está afeto aquela, logo, a conduta adotada pelas demandadas no caso em análise está abarcada pelo instituto do exercício regular de direito, não havendo que se falar na possibilidade de indenização ou de concessão de tutela inibitória. Improcedência da causa piloto que merece ser mantida pelo fundamento jurídico supracitado. Acolhido o incidente, fixada tese jurídica e negado provimento ao recurso no julgamento do processo-piloto. (BRASIL. Supremo Tribunal Federal. *Agravo em Recurso Extraordinário de n. 1307386*. Relatora Ministra Carmem Lucia. Disponível em: <http://stf.jus.br> . Acesso em: 15 abr. 2024).

Em sede de fundamentação do IRDR, foi destacada a licitude da atividade da proponente, que é uma ferramenta de pesquisa, e que apenas reproduz informações constantes no Diário Eletrônico, no seu exercício regular de um direito. Foi ressaltado também que a Constituição Federal, em seu art. 5º, inciso LX, consagra o caráter público do processo, sendo permitida a restrição da publicidade apenas nos casos em que a defesa da intimidade ou o interesse social o exigir.

Em voto divergente, ao tratar dos avanços tecnológicos, pontuou o Des. Carlos Eduardo Richinitti:

Tais modificações são típicas de nosso tempo, onde a cada dia renovam-se os arsenais tecnológicos e as múltiplas possibilidades de compartilhamento de dados a que a internet permite. Em épocas de superexposição, de arrefecimento das fronteiras entre público e privado, de vivência em uma sociedade chamada por alguns pensadores contemporâneos como a da superinformação – o que por um lado é absolutamente salutar – não se pode perder de vista determinados liames de proteção individual, sob pena de cancelar que se esteja tutelando não a liberdade de informação, mas a supercuriosidade.

Se um dado não é de interesse e utilidade coletiva, se diz respeito a uma condição apenas de determinado indivíduo, e se esse indivíduo não deseja que sua “ficha corrida” esteja ao alcance da comunidade mundial, por que razão esse dado deve ter seu conteúdo facilitado por empresas que exploram esse serviço como atividade econômica?

Qual o benefício de existir esse tipo de busca nominal em “sites” como, p. ex., Escavador e JusBrasil? A satisfação da curiosidade alheia? Atender uma demanda de mercado de empregadores que pretendem utilizar esse mecanismo em critérios de seleção ao invés de transparentemente solicitar uma certidão ao candidato? A busca por informações processuais para partes e advogados, atualmente, já é disponibilizada de modo rápido, fácil e seguro nos portais oficiais do Judiciário brasileiro. Esses mesmos portais, por sua vez, não permitem a pesquisa nominal para processos trabalhistas e criminais [...].

Após refletir sobre o assunto, o debate que ora proponho não é então sobre a licitude do conteúdo de determinada informação/conteúdo propriamente dito (até porque as fontes são diários oficiais), mas sobre um cidadão ter ou não a prerrogativa de, após

tomar conhecimento de vinculação da sua individualidade a processo judicial, com consequências potencialmente danosas, ver seu nome excluído da resposta de um ambiente virtual cujo objetivo é explorar comercialmente essa provedoria de pesquisas. Logo, essa pretensão está diretamente relacionada ao direito ao esquecimento, ferramenta de tutela da dignidade da pessoa humana.

Destaco que não se está falando da eliminação de conteúdo em si (pois é originalmente de um terceiro – os Diários Oficiais) tampouco de censura prévia por parte de provedores de pesquisa, mas que, se determinada pessoa se sente prejudicada com a disponibilização de mecanismos de busca nominais, após o crivo judicial, tenha a possibilidade de ver seu nome desindexado daquela plataforma. Como expus, tenho que não se pode confundir interesse público com curiosidade pública [...]

Assim, é evidente que alguém que tem vinculado a seu nome um processo criminal ou uma ação movida contra um ex-empregador conta com empecilhos que dificultam sobremaneira, quando não impedem, a obtenção de um posto de trabalho. Aqui, está-se falando de problema diretamente ligado ao seu direito de preservação da imagem, intimidade e vida privada (BRASIL, 1988, art. 5º, X).

Foi destacado ainda que, em que pese as informações decorram de órgãos públicos, as empresas provedoras de aplicação de internet incrementam tais informações por meio de algoritmos, tornando-as disponíveis no ambiente virtual de forma facilitada com a busca nominal, mediante verdadeiro tratamento de conteúdo.

Trata-se de um novo tratamento que não acompanha a finalidade originalmente vinculada a disponibilização dos dados no processo judicial.

Como vem sendo destacado neste estudo, isto se torna possível diante da vulnerabilidade dos dados inseridos nos processos judiciais.

Acompanhando o voto divergente, o Desembargador Eugênio Facchini Neto ainda ponderou:

Isso porque, numa sociedade que está longe do pleno emprego, informações pessoais, especialmente na esfera trabalhista, podem representar ser ou não aceito para uma vaga de trabalho. De fato, é um dado sociológico conhecido que muitos empregadores não apreciam empregados que ‘ousam’ reivindicar seus direitos junto à justiça laboral. O raciocínio é simples, quiçá simplório: “se um empregado ajuizou uma reclamatória trabalhista contra seu antigo empregador, ele talvez venha a fazer o mesmo comigo. Melhor não correr riscos. Vou empregar alguém que não revele disposição a reclamar”. Não sejamos ingênuos a imaginar que todas as reclamatórias trabalhistas são inevitavelmente justas e ‘honestas’. Mas inegavelmente que a maioria o é. E o efeito nefasto é exatamente esse: quem simplesmente reclama direitos que a legislação lhe outorga, diante do descumprimento dos deveres de seu empregador, pode acabar penalizado pela dificuldade de encontrar empregos futuros.

Contra a decisão que julgou o IRDR, foi interposto recurso extraordinário pela empresa responsável pelo sistema Escavador para ampliar os efeitos normativos da decisão em nome dos princípios da isonomia e da segurança jurídica.

Como o recurso não foi admitido, houve interposição de agravo, registrado sob o número ARE 1307386, perante o Supremo Tribunal Federal, que foi provido.

No acórdão, de relatoria do Ministro Luiz Fux, particularizando o caso em relação a outros já analisados na Suprema Corte, foi destacado que:

Referidos precedentes, no entanto, merecem distinção quanto ao caso sub examine, em que há peculiaridade de os dados pessoais disponibilizados em sítio de internet serem extraídos de publicação oficial do próprio Poder Judiciário e posteriormente tratados e compilados para busca inclusive pelo nome. In casu, o autor alega que a divulgação de seu nome vinculado a processos trabalhistas facilita a criação das chamadas listas sujas usadas por empregadores no âmbito da Justiça do Trabalho

[...]

De igual modo, há de se considerar que a solução da presente controvérsia, mediante o regime de precedentes qualificados, é essencial para garantir uniformidade, isonomia e coerência da jurisprudência constitucional e dar previsibilidade aos jurisdicionados, com a conseqüente diminuição das demandas massificadas. Configura-se, assim, a relevância da matéria sob as perspectivas social, econômica e jurídica (artigo 1.035, parágrafo 1º, do Código de Processo Civil), bem como a transcendência da questão cuja repercussão geral ora se submete ao escrutínio desta Suprema Corte. Nesse sentido, tenho que a controvérsia constitucional em apreço ultrapassa os interesses das partes, avultando-se relevante do ponto de vista econômico, político, social e jurídico.

Requereram ingresso como “*amicus curiae*” a Associação Brasileira de Lawtechs e Legaltechs (AB2L), Open Knowledge Brasil (OKBR), Defensoria Pública do Rio de Janeiro, Instituto Brasileiro de Política e Direito do Consumidor – Brasilcon, Google Brasil Internet Ltda, Associação Instituto Tornavoz, Associação Brasileira de Jornalismo Investigativo (ABRAJI), Instituto de Referência em Internet e Sociedade (IRIS), Instituto dos Advogados de São Paulo, dentre outras instituições.

A Procuradoria Geral da República apresentou parecer no sentido de que o referido tratamento adotado pelos portais de buscas seria ilegítimo, propondo a fixação das seguintes teses quanto à proteção de dados:

[...] II. O tratamento de dados pessoais de acesso público é condicionado à explicitação de propósitos legítimos e específicos que considerem a finalidade, a boa-fé e o interesse público que justificaram a sua disponibilização (art. 7º, §§ 3º e 7º, da LGPD), de modo que a transformação desses dados sem a devida fundamentação pode

ensejar responsabilização civil e administrativa do agente de tratamento (art. 42, da LGPD).

III. O tratamento de dados pessoais de acesso público por parte dos agentes de tratamento, de forma a permitir a publicização ampla e a consulta de informações de processos trabalhistas e criminais pelo nome das partes, além de exorbitar a autorização de tratamento de dados pela LGPD, tendo em conta a inexistência de justificção baseada em finalidade legítima e específica em concreto (arts. 7º, §§ 3º e 7º, e 10, da LGPD), viola os direitos fundamentais à privacidade, à intimidade, à inviolabilidade de dados e à autodeterminação informativa (art. 5º, X, XII e LXXIX, da CF).

IV. Presume-se a existência de dano moral se, após a solicitação de retirada feita pelo titular, a divulgação dos dados é mantida sem justificativa amparada na LGPD. (BRASIL. Supremo Tribunal Federal. *Agravo em Recurso Extraordinário de n. 1307386*. Relatora Ministra Carmem Lucia. Disponível em: <http://stf.jus.br>. Acesso em: 15 abr. 2024).

Segundo o referido parecer, os direitos fundamentais da privacidade e da proteção de dados são essenciais para o desenvolvimento da personalidade, decorrendo daí a autodeterminação informativa.

Foi frisado que o tratamento de dados pessoais de acesso público, disponibilizados por quem não é o titular, só é cabível caso observada a finalidade, a boa-fé e o interesse público, de modo a garantir os direitos do seu titular; e que a Resolução 121/2010 do CNJ e a Resolução 139/2014 do CSJT determinam que nos sites dos tribunais sejam aplicados recursos que impeçam a consulta ampla com base em dados pessoais em processos de natureza criminal e trabalhista, no intuito de evitar condutas discriminatórias<sup>48</sup>.

---

<sup>48</sup> Sobre o tema, Teffé (2022, p. 49) pondera: “Diante disso, não mais parece fazer sentido considerar um dado ou um conjunto de dados de forma isolada ou estática, mas, sim, dentro de uma perspectiva dinâmica que considere diversos fatores e sujeitos. Entretanto, tal perspectiva deve levar em conta, também, a necessidade de não ocorrer um alargamento excessivo da categoria dos dados sensíveis, já que isso tanto limitaria uma série de tratamentos e bases legais importantes para os agentes quanto deixaria da categoria com menos relevo e valor no futuro, diante de uma possível banalização. Como forma de concretização da dignidade da pessoa humana, e figurando como direito da personalidade, a proteção de dados pessoais revela-se fundamental, sendo condição para que o sujeito se realize e se relacione em sociedade. Como apresentado, tutelar dados sensíveis e tratamentos de caráter sensível significa proteger a pessoa contra discriminações abusivas ou ilícitas, assegurar igualdade material no seu tratamento e permitir o livre desenvolvimento da sua personalidade, levando-se em conta suas diferenças e características particulares”.

Trata-se de uma espécie de pseudoanonimização<sup>49</sup> para garantir a intimidade e privacidade<sup>50</sup> das pessoas e evitar a ocorrência de práticas discriminatórias.

Como já apontado neste estudo, em tópicos antecedentes, alguns sites de aplicação de internet, ao realizarem o tratamento de informações extraídas dos tribunais, possibilitam, muito embora todo o esforço empregado pelo Conselho Nacional de Justiça, a consulta pública de processos trabalhistas e criminais com os dados pessoais, o que violaria os direitos da personalidade.

Inclusive, por meio destes sistemas de buscas, fatos da vida de uma pessoa, que são do âmbito privado e que não são efetivamente de interesse público, podem ser localizados com uma simples pesquisa por nome. Isto faz com que qualquer usuário tenha acesso a diversas informações sobre as pessoas.

Em que pese seja possível utilizar-se de informações dos processos para finalidades diversas das que justificaram a publicação pelos Diários Oficiais, o agente de tratamento só pode realizar tratamento para propósitos legítimos, considerando a boa-fé, a finalidade e o interesse público que ampararam a divulgação. No entanto, como se sabe, isto não está sendo respeitado em muitas situações, como resta evidenciado pelo caso em análise.

A disponibilização das informações relacionadas aos processos judiciais decorre de previsão constitucional que visa prestigiar a ampla transparência e publicidade<sup>51</sup>, sendo que a

---

<sup>49</sup> Bioni (2020, p. 44) esclarece, no que se refere à pseudoanonimização, que: “Neste cenário, o próprio agente tem informações adicionais, ainda que mantidas separadamente, para reverter o processo de anonimização, ou seja, ele possui meios próprios para transmutar um dado aparentemente anonimizado em um dado pessoal, o que é revelado com base em uma análise subjetiva focada na sua própria capacidade de entropia de informação. O cenário supradescrito é o que se convencionou chamar de pseudoanonimização, isto é, uma falsa, superficial, técnica de anonimização que é quebrável em especial pela própria organização que a empregou”.

<sup>50</sup> No relatório da análise realizada sobre o tratamento de dados pessoais na consulta de jurisprudência, pontuou o CNJ (2021, p. 11) que: “Assim, 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 Victor Nunes Leal para V.N.L); • 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.: de 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)”.

<sup>51</sup> Sobre a transparência e publicidade, pontuam Bulzico e Sousa (2022, fls. 155): “Assim, com a atenção voltada ao atropelo de direitos fundamentais dos titulares desses dados, conectado aos direitos à privacidade, intimidade e



lei somente pode restringi-la em hipóteses nas quais a intimidade ou o interesse social justificarem a não divulgação.

Ocorre que estes sites de aplicação possibilitam a utilização de meios de busca que não são admitidos pelos próprios sites dos órgãos públicos<sup>52</sup>, que vedam, com base em resoluções do Conselho Nacional de Justiça, a busca em processos trabalhistas e criminais por meio de dados pessoais.

Nesta linha, os que defendem as atividades desempenhadas por estas plataformas sustentam que, embora as informações públicas estejam disponibilizadas pelos portais dos

---

sigilo (art. 5º, incisos X e XII, CF/1988) na publicização em processos judiciais, preocupa-se, primeiramente, fazer uma distinção terminológica entre “publicidade” e “transparência”, que por vezes são consideradas sinônimas. Nas palavras de Jorge Hage, a transparência pode ser definida como a atuação do órgão público no sentido de tornar a sua conduta cotidiana, e os dados dela decorrentes, acessíveis ao público em geral. Somente a partir dos anos 2000 o “Princípio da Transparência” passou a ser elencado em diversos diplomas normativos, a exemplo do art. 2º da Lei de Responsabilidade Fiscal (Lei Complementar n.º 101/00), art. 4º da Lei de Proteção ao Usuário do Serviço Público (Lei n.º 13.460/2017) e na própria Constituição Federal, em emendas recentes (Emenda Constitucional 103/2019). Por sua vez, também como elemento de sustentação da relação de confiança entre cidadão e Estado, a publicidade encontra-se prevista no art. 37 da Constituição Federal e se apresenta como princípio da Administração Pública e uma das principais ferramentas para que o cidadão participe ativamente da democracia, tomando ciência dos atos governamentais e assim possibilitando fiscalizar os representantes do Estado. Importante ressaltar que a publicidade abre possibilidades de conhecimento, para além das informações relacionadas aos “atos da Administração” que sejam criadas, coletadas e armazenadas pelo Estado com finalidade do controle democrático, mas alcança, ainda, informações coletadas ou meramente armazenadas pelo Estado em outras redes de acesso, a exemplo do processo judicial eletrônico. É claro que há uma forte relação entre os elementos distinguidos acima, contudo restou demonstrado que não se trata de palavras sinônimas, pois eventual confusão entre elas pode gerar risco anacrônico. Ao desenhar o cenário atual com a proteção de dados pessoais, inserido no mesmo contexto de privacidade à identidade do titular desses dados, certamente faz-se necessário observar o arcabouço normativo para definir qual das possibilidades invocadas pela publicidade perseguir. Se utilizada como norma de conduta ao controle constitucional, a publicidade torna-se regra primária de comportamento; contudo, se utilizada como condição de validade e eficácia, pode ser utilizada como ferramenta de derivação de outras normas”.

<sup>52</sup> No relatório da análise realizada sobre o tratamento de dados pessoais na consulta de jurisprudência, pontuou o CNJ (2021, p. 14) que: “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 (assim considerados, entre outros, os nomes das partes e de seus advogados, o número de identificação das partes no cadastro federal de contribuintes e 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 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 n.º 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 n.º 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). 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.”

governos, nem sempre estão acessíveis, motivo pelo qual seria válida a atividade desempenhada pelas plataformas por facilitar o acesso às informações.<sup>53</sup>

Muito embora não alterem o conteúdo das publicações oficiais, o tratamento realizado por estas empresas não leva em consideração a finalidade, a boa-fé e o interesse público, assim como violam a privacidade e a intimidade.

Inclusive, por meio da realização deste tratamento, os sistemas podem traçar um perfil virtual da pessoa<sup>54</sup>, passível de comercialização<sup>55</sup>, o que já foi pontuado neste estudo.

Este estudo se filia ao entendimento de que inexistente interesse público neste tipo de cruzamento de informações realizadas por sistemas desta natureza, não havendo justificativa ao amplo acesso a dados pessoais sem o consentimento do titular.

---

<sup>53</sup> No requerimento para admissão como *Amicus Curiae*, asseverou a Associação Brasileira de Jornalismo Investigativo (IBRAJI) que: “A coleta, o manejo e a disponibilização de dados processuais como os que são feitos pelo recorrente, assim como pela iniciativa privada como um todo, ampliam o livre fluxo da informação. Os dados tratados que, vale lembrar, são públicos, auxiliam os operadores do direito, por óbvio, mas igualmente facilitam a pesquisa, a classificação e o cruzamento de informações por jornalistas que depois irão publicá-las sob a forma de notícias. A pesquisa manual desses dados, tradicionalmente feita na plataforma dos Tribunais do país é tarefa hercúlea, de tão complexa. Há atualmente 10 sistemas de acesso a processos judiciais em uso no Brasil, e às vezes um mesmo Estado adota mais de um sistema. A dificuldade é imensa, porque os Tribunais por vezes adotam versões diferentes de um mesmo sistema, de sorte que, embora alguns sistemas sejam compartilhados, a dificuldade de acesso é multiplicada em razão das diversas versões utilizadas” (p. 3) e “O resultado do julgamento deste recurso tem potencial para alterar significativamente o cenário da liberdade de expressão no país. Se restar decidido que empresas que exercem tratamento de dados de processos judiciais não poderão mais fazê-lo, haverá restrição ao acesso a informações que já são públicas, mas que atualmente estão acobertadas por burocráticos sistemas, afetando-se um número indeterminado de cidadãos” (p. 9-10).

<sup>54</sup> No relatório da análise realizada sobre o tratamento de dados pessoais na consulta de jurisprudência, pontuou o CNJ (2021, p. 14) que: “Por fim, 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. Para exemplificar: mesmo que um(a) magistrado(a), cioso(a) do princípio da necessidade, tenha o cuidado, ao redigir sua decisão, de pseudonimizar dados de determinada parte processual por considerá-los impertinentes, desproporcionais ou excessivos, ainda assim o nome dessa parte constará do Diário da Justiça eletrônico, dos sistemas de acompanhamento processual e dos repositórios públicos de jurisprudência mantidos pelo tribunal ou por entidades privadas na rede mundial de computadores. Em uma situação como essa, o esforço de pseudonimização não seria suficiente para evitar a associação entre as informações contidas na decisão judicial e o titular dos dados pessoais que se desejava proteger”.

<sup>55</sup> Inclusive, nos autos do agravo de n. 1.307.386/RS, após análise das atividades desempenhadas pelo site Escavador e descrição das condições de uso e finalidade da plataforma, a manifestação do *Amicus Curiae* Defensoria Pública do Estado do Rio de Janeiro destacou que: “a plataforma da recorrente não se destina a auxiliar na prestação da tutela jurisdicional, mas à consecução das atividades empresárias e, por consequência, ao lucro e à otimização dos negócios de terceiros.” Já quanto ao site *JusBrasil*, a manifestação do *Amicus Curiae* Defensoria Pública do Estado do Rio de Janeiro alertou que “plataforma compartilha dados pessoais com terceiros indeterminados e tem finalidades muito distintas daquela que motivou a publicização dos dados pessoais dos jurisdicionados, quando postularam a prestação da tutela jurisdicional”.

Os dados pessoais de acesso público, disponibilizados em processos judiciais, têm por finalidade a prestação da tutela jurisdicional, que é um serviço público essencial, e não a atividade lucrativa de particulares.

Ademais, tal tratamento de dados de acesso público, que possibilita ampla publicização e a consulta a informações relacionadas a processos trabalhistas e criminais pelo nome das partes, normalmente está associado a outros serviços ofertados e comercializados por estas empresas em suas plataformas, o que evidencia aparente desvirtuamento da finalidade que justificou a divulgação dos dados dos sujeitos processuais, infringindo o parágrafo 7º do art. 7º da LGPD.

Afinal, este tratamento não é compatível com a finalidade e interesse que justificaram a publicização dos dados, qual seja, a prestação jurisdicional.

Por violar a proteção de dados, esta atividade pode gerar danos ao titular das informações, já que atinge os direitos da personalidade, em especial, o direito à privacidade, à autodeterminação e à intimidade, comprometendo o livre desenvolvimento da personalidade, sendo presumida a existência de danos quando tenha ocorrido a manutenção indevida dos dados após prévia solicitação de retirada pelo titular nos termos do parecer.

O julgamento do referido tema pelo Supremo Tribunal Federal apontará um importante caminho para a proteção de dados em processos judiciais no Brasil.

No entanto, diante da indefinição deste cenário e da situação de vulnerabilidade dos dados pessoais, já que o mencionado processo encontra-se pendente de julgamento, sem data prevista para inclusão em pauta, mostra-se reforçada a necessidade de imposição de parâmetros para restrição de acesso aos dados pessoais contidos nos processos judiciais, especialmente, diante dos riscos a que estes estão submetidos.

### 3.3 A AFETAÇÃO À AUTODETERMINAÇÃO EM DECORRÊNCIA DE INTERESSE PÚBLICO E MEDIANTE DEFINIÇÃO DE REGRAS: O ACÓRDÃO 403.215 DO STJ DE PORTUGAL

Como visto nos tópicos anteriores, as discussões judiciais sobre assuntos relacionados a este estudo ainda estão em curso no Brasil, restando caracterizado um cenário de indefinições.

Na Europa, em que pese os desafios que envolvam estes assuntos sejam grandes, as reflexões sobre a proteção de dados já se encontram mais avançadas.

Ademais, como a Lei Geral de Proteção de Dados brasileira se inspirou no Regulamento Geral sobre Proteção de Dados (em inglês, GDPR - *General Data Protection Regulation*)<sup>56</sup> da Europa, que é a principal regulamentação sobre a proteção de dados e identidade dos cidadãos da União Europeia, uma análise desta natureza mostra-se viável, sendo possível se extrair da experiência europeia algumas soluções normativas e judiciais que podem ser úteis para resolução de questões também vivenciadas no Brasil<sup>57</sup>.

Nesta linha, este estudo buscou no sistema jurídico português algumas destas soluções para amparar as propostas que serão defendidas.

A questão de dados já vem sendo discutida há muito em Portugal. Sobre o tema, pontua Teixeira (2019, p. 1) que, desde 1976, a Constituição da República Portuguesa<sup>58</sup> já traz previsões sobre o tema e que:

---

<sup>56</sup> Neste particular, Oliveira e Silva (2023, p. 11) ponderam que: “Como a LGPD brasileira teve forte influência da legislação europeia, importante o estudo preliminar sobre a regulamentação da questão dada pelo General Data Protection Regulation (GDPR) ao tratamento de dados feitos pelo Poder Judiciário no ambiente da União Europeia. Em seu considerando n. 20, o GDPR destacou que sua regulamentação também é aplicável às atividades dos Tribunais, mas afastou a competência das autoridades de controle sobre o tratamento de dados pessoais feito pelos tribunais no exercício da sua função jurisdicional, objetivando assegurar a independência do Judiciário no exercício da sua função jurisdicional, nomeadamente a tomada de decisões. Além disso, a alínea “a” do item 1 do art. 37 do GDPR dispensa a designação de encarregado de proteção de dados nos casos em que o tratamento for feito pelos tribunais no exercício de suas atividades jurisdicionais. O item 3 do art. 55 do GDPR ratifica que as autoridades de controle não têm competência para fiscalização das operações de tratamento efetuadas pelos tribunais no exercício da sua função jurisdicional”.

<sup>57</sup> Analisando recente precedente do Tribunal de Justiça da União Europeia, Faleiros Junior comentou sobre a convergência entre a RGPD e a LGPD, bem como sobre a importância dos julgamentos europeus nas interpretações e aplicações da LGPD no Brasil (2024, p. 1): “A decisão do TJUE no Processo C-590/22 não apenas harmoniza a aplicação do RGPD entre os Estados-membros da União Europeia, promovendo segurança jurídica, mas também serve de referência para futuras interpretações e aplicações da LGPD no Brasil. Inegavelmente, a convergência entre essas legislações poderá fortalecer a proteção de dados pessoais, oferecendo um caminho claro para a responsabilidade civil e estimulando novas reflexões sobre a aplicação das regras de responsabilização em contextos diversos”.

<sup>58</sup> Oliveira e Silva (2023, p. 12) ponderam que: “Em Portugal, o art. 206 da Constituição da República prevê, de forma semelhante ao Brasil, que as audiências dos tribunais serão públicas, salvo quando o próprio tribunal decidir o contrário, em decisão fundamentada, para salvaguarda da dignidade das pessoas e da moral pública ou para

“Não sendo uma problemática nova, a razão para as recentes alterações legislativas e para a as actuais preocupações prende-se naturalmente com as novas tecnologias informáticas de recolha e tratamento de dados em massa, que eram impensáveis à data, nomeadamente o chamado Big Data” e que “É esta possibilidade que o acesso e tratamento informático em massa dos dados agora permite, e que actualmente já é possível no âmbito dos processos judiciais, que suscita novas problemáticas que merecem a nossa atenção, nomeadamente naqueles em que se aplica o Código de Processo Civil”.

A escolha do sistema jurídico português se justifica, dentre outras razões, pela grande proximidade existente entre institutos previstos em ambos os ordenamentos e pelo momento vivido em ambos os sistemas judiciais.

Neste sentido, entende Masseno (2021, p. 2) que:

“Em matéria de tratamento de dados pessoais nos respetivos sistemas judiciais, os Ordenamentos português e brasileiro passam por vicissitudes semelhantes, ainda que em termos simétricos. Assim, ambos assentam em regimes gerais, os dispostos pelo 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) RGPD, e pela Lei n.º 13.709, de 14 agosto de 2018, Lei Geral de Proteção de Dados Pessoais LGPD, de cujo âmbito objetivo excluem a justiça criminal (Art.ºs 2.º n.º 1, 9.º n.º 1 f), 37.º n.º 1 a) e 55.º n.º 3, bem como o Considerando 20, do RGPD e Arts. 1º e 4º III d), este a contrario, da LGPD). Com efeito, para o tratamento de tais dados estão previstas disciplinas próprias. Em Portugal, pela Lei n.º 59/2019, de 8 de agosto, que aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais (transpondo a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho), no Brasil ainda estando por efetivar (Art. 4º III d) da LGPD)”.

---

garantir o seu normal funcionamento. O art. 164.º, n.º 3, do Código de Processo Civil de Portugal, estabelece que: “O acesso à informação do processo também pode ser limitado, em respeito pelo regime legal de proteção e tratamento de dados pessoais, quando, estando em causa dados pessoais constantes do processo, os mesmos não sejam pertinentes para a justa composição do litígio”. A lei n.º 32/2009, estabelece o regime jurídico aplicável ao tratamento de dados referentes ao sistema judicial em Portugal, sendo que, na base de dados das pesquisas jurisprudenciais, é possível a identificação do nome dos julgadores e, com relação às partes, se elas forem pessoas físicas, são apontadas apenas as suas iniciais, preservando-se a sua privacidade.”

É certo, no entanto, que, por mais que exista proximidade entre institutos, a análise comparativa de questões que envolvem ordenamentos jurídicos diversos é desafiadora<sup>59</sup>.

Neste sentido, este estudo buscou colher ideias e preceitos gerais da experiência europeia, refletida em dois julgados portugueses, que pudessem auxiliar em questões também vivenciadas no Brasil.

O primeiro Acórdão analisado, qual seja, o de n. 403/2015, trata do tema afetação à autodeterminação em decorrência de interesse.

O Acórdão de n. 403/2015, proferido pelo Supremo Tribunal de Justiça de Portugal, no processo de n. 773/15, analisou a constitucionalidade de dispositivo contido no “Regime Jurídico do Sistema de Informações da República Portuguesa”, que autoriza o compartilhamento, dentro de um contexto de combate ao terrorismo, de informação bancária, fiscal, de tráfego, de localização e outros dados relacionados a comunicações para identificar o usuário, a fonte, o destino, a data a hora e o tipo de comunicação “sempre que necessárias, adequadas ou proporcionais, numa sociedade democrática, para cumprimento das atribuições legais dos serviços de informações, mediante autorização prévia e obrigatória da Comissão de Controle Prévio”.

Trata-se de tema relacionado ao tratamento de dados decorrente do sistema de comunicação e que analisa a afetação da autodeterminação informativa em decorrência de interesse público e mediante definição de regras claras, questão relevante para o objeto da análise deste trabalho.

A questão analisada pelo Supremo Tribunal de Justiça de Portugal residia em saber se a norma que tratava da ameaça à segurança nacional estaria adequada ao sistema de privacidade

---

<sup>59</sup> Sobre o tema, entende ainda Masseno (2021, p. 8) que: “Em Portugal e no Brasil, os tratamentos de dados pessoais nos respectivos Sistemas Judiciais estão passando por transformações profundas, também no que se refere às questões respeitantes à segurança. Para além de questões comuns, como a da previsão no RGPD e na LGPD de regimes jurídicos próprios para a Justiça Criminal, uma diferença marcante é evidenciada, a do controle dos meios operacionais afetos à Justiça por parte do Poder Executivo em Portugal. Ora, com especial uma especial incidência no que se refere à segurança no tratamento dos dados, a opção legislativa no sentido de não atribuir tais responsabilidades aos Órgãos do Poder Judiciário, incluindo o Conselho Superior da Magistratura e o Conselho Superior dos Tribunais Administrativos e Fiscais, afasta radicalmente as soluções regulatórias e operacionais de ambos os países, por muito semelhantes que sejam o RGPD e o LGPD”.

das telecomunicações, que proíbe, naquele país, a ingerência das autoridades públicas nos meios de comunicação.

Após analisar a evolução histórica do regime jurídico do sistema de informações da República Portuguesa, responsável pelo tratamento de informações necessárias à salvaguarda da independência nacional e à garantia da segurança interna, o acórdão destacou que a finalidade do dispositivo contido no Decreto n. 426/XII era a prevenção de terrorismo, espionagem, sabotagem e criminalidade organizada, devendo as medidas previstas serem adequadas, necessárias e proporcionais para atingirem a sua finalidade, por se tratar de uma sociedade democrática.

A autorização para se ter acesso às informações necessárias, que compreenderiam dados de base, localização e tráfego, deveria ser concedida por uma Comissão composta por três juízes, que consideraria a reserva da intimidade da vida privada.

O acesso pretendido era sobre metadados relativos às circunstâncias em que a comunicação foi realizada (dados de tráfego/de utilização), e não sobre o conteúdo da comunicação (dados de conteúdo).

Foi apontado o risco de violação dos direitos fundamentais dos participantes no ato comunicacional, já que, por meio destes dados, é possível traçar um perfil sobre o indivíduo, revelando as pessoas com quem mais conversa, os locais que mais visita e os respectivos horários.

Foi ressaltado que tais informações são, em muitas situações, mais importantes que o próprio conteúdo do ato de comunicação, de modo que a manipulação indevida pode violar o desenvolvimento da personalidade, em especial, na liberdade da ação, na privacidade e na autodeterminação informativa.

Neste sentido, pontua o acórdão (PORTUGAL, 2015):

Desde logo, a *liberdade de ação*, enquanto vertente do direito ao desenvolvimento da personalidade, de acordo com a qual, na interação com os outros, a condução da vida de cada um é *autoconformada* pela sua atuação, o que pressupõe, como referem Gomes Canotilho e Vital Moreira «a exigência de *proibição de ingerências* dos poderes públicos (...) como, por exemplo, (...) “o direito a não ser espiado”» (*Constituição da República Portuguesa Anotada*, 2.<sup>a</sup> ed., Vol. I, pág. 465).

Depois, com a *esfera íntima* e a *esfera privada* da pessoa humana, seja enquanto pretensão de isolamento, tranquilidade e exclusão do acesso dos outros a si próprio (*direito à solidão*), seja, enquanto impedimento à ingerência dos outros (*direito ao anonimato*), seja ainda, mais modernamente, e perante a insuficiência protetora das referidas dimensões, enquanto controlo das informações que lhe dizem respeito e de subtração ao conhecimento dos outros os factos reveladores do modo de ser do sujeito na condução da sua vida privada (*autodeterminação informacional*). Como refere Joaquim Sousa Ribeiro, esta última dimensão, hoje a de maior relevo, «impede que o “eu” seja objeto de apropriação pelos outros, como matéria de comunicação na esfera pública. Nela conjuga-se o *direito ao segredo* (à intromissão dos outros na esfera privada, com tomada de conhecimento de aspetos a ela referentes) e um *direito à reserva* (proibição de revelação)» – cfr. *A Tutela de bens da personalidade na Constituição e na Jurisprudência constitucional portuguesas, in Estudos de Homenagem ao Prof. Doutor José Joaquim Gomes Canotilho, Vol. III, Coimbra Editora, p. 853*).

O acórdão destacou, também, que o progresso tecnológico, ao disponibilizar meios poderosos de tratamento de dados, aumentou consideravelmente as possibilidades de devassa.

A autodeterminação informativa, por sua vez, deve garantir o segredo e a liberdade de se comunicar, sendo que a privacidade da comunicação abrange não apenas a proibição de interferência, como também a impossibilidade de acesso posterior às condições fáticas em que ocorreu a comunicação.

Ressaltou-se que somente há sacrifício do direito à inviolabilidade das comunicações privadas, um direito fundamental, na investigação criminal perante um caso concreto, quando autorizada pelo judiciário, com base na necessidade, adequação e proporcionalidade, na busca da verdade real em nome da justiça e da segurança. Ou seja, a priori, o âmbito da não ingerência nas telecomunicações está constitucionalmente delimitado.

Ocorre que, nos termos do art. 2º do art. 78 do Decreto 426/XII, a atuação dos oficiais de informação no tratamento previsto não estaria dentro do âmbito da investigação criminal, pois se trataria de coleta de informações para efeito de prevenção da ocorrência de sabotagem, espionagem, terrorismo, criminalidade organizada e prática de atos que possam alterar o Estado Democrático de Direito.

A coleta de informações para a adoção de medidas preventivas não é atividade inerente à investigação criminal, segundo o próprio acórdão, e sim procedimentos administrativos que não atendem os princípios do processo penal.

Ademais, ainda que composto por juízes, a Comissão de Controle Prévio tem natureza de órgão administrativo e não exerce a função jurisdicional.



Ainda que não fosse assim, a norma precisaria prever – mas não o faz – a forma de acesso, a duração de acesso e a eliminação dos dados de tráfego coletados sob pena de falta de segurança jurídica e em desrespeito ao direito ao esquecimento.

Neste sentido, pontua o acórdão:

Desta jurisprudência decorrem, pois, várias exigências para uma norma que, como a presente, permita o acesso a dados de tráfego das comunicações de indivíduos sem o seu consentimento ou conhecimento. Em primeiro lugar, a lei deve empregar *termos suficientemente claros* para possibilitar a todos os cidadãos terem conhecimento das circunstâncias e dos requisitos que permitem ao poder público aceder aos dados em causa, sendo que os requisitos para o efeito devem ser claramente determinados; deve ainda fazer menção, com precisão, dos *casos específicos* em que o acesso deve ter lugar, prever a fixação de um *limite de duração* da medida, e das regras e prazos para eliminação dos dados de tráfego. Só assim se poderá falar de uma ingerência determinável e que garanta segurança jurídica aos interessados.

Mas, se assim é, há que reconhecer que, para além da impossibilidade de compatibilização com a norma do n.º 4 do artigo 34.º da CRP, a norma do n.º 2 do artigo 78.º do Decreto n.º 426/XII não contém *densidade suficiente* para, num domínio de lei restritiva, possibilitar a fiscalização da legalidade e a defesa dos direitos e interesses dos cidadãos. Com efeito, a norma não satisfaz suficientemente, como contrapartida do acesso aos dados de tráfego, as exigências de determinabilidade que são garantidas em matéria de processo criminal, devolvendo para a esfera administrativa ponderações que deveriam constar da lei.

[...]

Note-se que, em contrapartida, a Lei n.º 32/2008, que não se aplica aos sistemas de informação, estabelece requisitos muito mais precisos para o acesso à informação em contexto de processo penal, ao prever, no artigo 9.º, n.º 1, que «a transmissão dos dados referentes às categorias previstas no artigo 4.º só pode ser autorizada [...] se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter no âmbito da investigação, deteção e repressão de crimes graves. (PORTUGAL. Supremo Tribunal de Justiça. *Acórdão n.º 720/2022*. Processo n. 836/21. Plenário. Relator: Conselheiro Lino Rodrigues Ribeiro. Julgamento em 3 de novembro de 2022. Disponível em: [www.stj.pt](http://www.stj.pt). Acesso em: 29 abr. 2024).

Outra questão a ser ponderada é que o decreto possibilita que haja o acesso a informações sem que sequer haja um alvo em concreto, buscando detectar padrões de conduta de uma forma ampla.

Neste cenário de insegurança jurídica, o Supremo Tribunal de Justiça de Portugal decidiu pela inconstitucionalidade da norma de n. 2, do art. 78, do Decreto n. 426/XII da Assembleia da República Portuguesa, que aprovava o regimento jurídico do sistema de informações de Portugal.

Tal precedente, proveniente de tribunal superior estrangeiro, evidencia a preocupação e a atenção que deve ser dirigida ao controle de tratamento de dados, num momento de avanço tecnológico, no intuito de preservar a autodeterminação informativa e a privacidade.

Em razão da indefinição de critérios objetivos sobre a forma de acesso, de duração e de eliminação de dados coletados, foi considerada inconstitucional a norma que admitia acesso a dados de comunicação numa situação de violação da comunicação.

É possível traçar um paralelo em relação à questão da publicidade ampla e indistinta dos dados processuais no Brasil, posto que a ampla possibilidade de acesso a estes dados no Brasil viola a autodeterminação informativa, já que não existem regras claras sobre o tratamento por pessoas que acessam o conteúdo dos atos processuais, pondo em risco o livre desenvolvimento da personalidade por violação ao direito de privacidade.

A vulnerabilidade dos dados expostos nos processos judiciais pode permitir que ocorram tratamentos desautorizados, alheios à finalidade e que podem gerar dados aos seus titulares.

O ordenamento jurídico brasileiro, efetivamente, não traz regras que disciplinem a duração do acesso e de eliminação de dados coletados por meio dos autos dos processos judiciais.

Neste cenário, faz-se necessário a instituição de parâmetros para a definição de regras de acesso aos dados pessoais, em níveis de publicidade, na tentativa de salvaguardar os dados pessoais existentes nos processos judiciais.

#### 3.4 A PUBLICIDADE DE ATOS DE PROCESSO COM PESSOAS COM INCAPACIDADE: O ACÓRDÃO 720.2022 DO STJ DE PORTUGAL

O outro precedente que merece destaque, também proveniente do Supremo Tribunal de Justiça de Portugal, seguindo o quanto apontado no tópico anterior, é aquele proferido no Processo de número 836/21, por meio do acórdão de número 720/2022, de relatoria do Conselheiro Lino Rodrigues Ribeiro, e que trata da publicidade de atos de processo que envolve pessoas com incapacidade.

O acórdão analisou recurso interposto pelo Ministério Público contra decisão no sentido de que a publicidade<sup>60</sup>, no caso de “regime jurídico do maior acompanhado” – que substituiu os institutos da interdição e inabilitação em Portugal, numa mudança paradigmática de substituição para acompanhamento - de pessoas com incapacidade, seria apenas de interesse do comércio jurídico.

O juízo originário entendeu que, nestes casos, o conteúdo do ato processual publicado compromete os dados pessoais ao revelar a sua condição, motivo pelo qual entendeu inconstitucional a norma que previa a possibilidade de publicidade, por violar o direito à autodeterminação informacional, que tem ligação direta com o direito de livre desenvolvimento da personalidade e por tratamento discriminatório da pessoa com deficiência.

O referido caso analisa o artigo 153 do Código Civil Português, a saber:

A publicidade a dar ao início, ao decurso e à decisão final do processo de acompanhamento é limitada ao estritamente necessário para defender os interesses do beneficiário ou de terceiros, sendo decidida, em cada caso, pelo tribunal (PORTUGAL, 1966, art. 1).

---

<sup>60</sup> Sobre a questão do tratamento informático dos processos e a publicidade no direito português, pontua Teixeira (2019, p. 4): “O DL n.º 97/2019, de 26/07 introduziu alterações relevantes nas normas do Código de Processo Civil relacionadas com o tratamento informático dos processos e com a sua publicidade, que convocam novos desafios de conjugação do mesmo com o RGPD, exigindo quer às Secretarias Judiciais, quer aos Magistrados Judiciais deveres acrescidos de verificação da concordância entre a publicidade dos processos e o RGPD”. Neste particular, Teixeira (2019, p. 4) aponta previsão contida no código de processo civil português, no que se refere a limitações à publicidade do processo: “1 - O acesso aos autos é limitado nos casos em que a divulgação do seu conteúdo possa causar dano à dignidade das pessoas, à intimidade da vida privada ou familiar ou à moral pública, ou pôr em causa a eficácia da decisão a proferir. 2 - Preenchem, designadamente, as restrições à publicidade previstas no número anterior: a) Os processos de anulação de casamento, divórcio, separação de pessoas e bens e os que respeitem ao estabelecimento ou impugnação de paternidade, a que apenas podem ter acesso as partes e os seus mandatários; b) Os procedimentos cautelares pendentes, que só podem ser facultados aos requerentes e seus mandatários e aos requeridos e respetivos mandatários, quando devam ser ouvidos antes de ordenada a providência; c) Os processos de execução só podem ser facultados aos executados e respetivos mandatários após a citação ou, nos casos previstos no artigo 626.º, após a notificação; independentemente da citação ou da notificação, é vedado aos executados e respetivos mandatários o acesso à informação relativa aos bens indicados pelo exequente para penhora e aos atos instrutórios da mesma. d) Os processos de acompanhamento de maior. 3 - O acesso a informação do processo também pode ser limitado, em respeito pelo regime legal de proteção e tratamento de dados pessoais, quando, estando em causa dados pessoais constantes do processo, os mesmos não sejam pertinentes para a justa composição do litígio. – este número foi introduzido pelo DL n.º 97/2019, de 26/07”.

Examina, também, o artigo 893, n. 1, do CPC: “O juiz decide, em face do caso, que tipo de publicidade deve ser dada ao início, ao decurso e à decisão final do processo”. Ambos os artigos disciplinam a publicidade do processo de “acompanhamento” de maior.

Antes, como a interdição e a inabilitação determinavam a incapacidade para realizar atos de disposição de patrimônio, as ações tinham publicização obrigatória, incluindo publicação de edital e registro da sentença de interdição perante o registro civil.

No caso do acompanhamento, destacou o acórdão que é limitado ao necessário, preservando a capacidade até o limite, sendo que o tribunal tem uma flexibilidade nas providências a serem adotadas, com base na razoabilidade e na oportunidade.

Nesta linha, a forma de publicidade acerca do início, do decurso e da decisão final também é flexível e se limita ao estritamente necessário para atender o interesse do acompanhado ou de terceiros, sendo que o tipo de publicização da ação é conformado pelo tribunal. Deve haver a publicidade, em especial, por conta da anulabilidade dos atos praticados pelo acompanhado.

No caso concreto, é verificada a necessidade de dar publicização à ação e a escolha de meios adequados, permitindo ao juiz determinar, a depender da vulnerabilidade, o que é estritamente necessário para a defesa do interesse do acompanhado e de terceiros.

Neste particular, pontuou o acórdão:

E, conseqüentemente, considerar a publicização da ação tanto mais premente quanto mais impossibilitada se encontrar a pessoa em questão de governar os seus bens, mais expressivo for o seu património, mais intensa se revelar a sua atividade económica e, sobretudo, mais conjeturável se apresentar a possibilidade de aplicação no caso concreto de uma medida de acompanhamento com impacto sobre a capacidade para o exercício de direitos patrimoniais; e, inversamente, tanto mais dispensável quanto menos afetada se apresentar a capacidade para querer e entender do beneficiário, menos significativo for o seu património ou o seu nível de interação negocial e, sobretudo, menos antecipável for a hipótese de vir a ser cometida ao acompanhante a representação do acompanhado, a administração total ou parcial dos respetivos bens ou a autorização para a prática de atos pertinentes ao governo dos mesmos (artigo 145.º, n.º 1, alíneas *b*), *c*) e *d*), do CC). Prescindindo o legislador de uma *ponderação em abstracto*, confiou-se assim ao juiz a decisão sobre o *grau* e *formas* de publicização da ação, permitindo-lhe dessa forma conformá-la e adequá-la às condicionantes próprias e específicas de cada caso, tal como indiciadas pelos factos alegados e tipo de proteção requerido na petição inicial, quando se trate de aferir da publicidade a dar ao início da ação (artigo 892.º, n.º 1, alíneas *a*) e *b*), do CPC); e às forem sendo conhecidas no decurso do processo, quando se imponha uma atualização ou uma renovação daquele juízo preliminar em face dos novos elementos entretanto carreados para os autos (artigo 897.º do CPC) ou até mesmo da adoção de medidas de acompanhamento provisórias ou cautelares (artigos 139.º, n.º 2, do CC, 891.º, n.º 2, do CPC).

Por último, na senda ainda do compromisso com a adoção de um regime vinculado ao «*respeito pela privacidade*» das pessoas com deficiência (v. supra, o n.º 9), abandonou-se a publicitação obrigatória da ação através de anúncios e editais que caracterizava os processos de interdição e inabilitação, levando em conta que se tratava de meio potencialmente vexatório e estigmatizante para visado e, em última análise, potencialmente dissuasor do recurso a este tipo de ações de modo a evitar os danos colaterais que a publicidade representava. (PORTUGAL. Supremo Tribunal de Justiça. *Acórdão n.º 720/2022*. Processo n. 836/21. Plenário. Relator: Conselheiro Lino Rodrigues Ribeiro. Julgamento em 3 de novembro de 2022. Disponível em: [www.stj.pt](http://www.stj.pt). Acesso em: 29 abr. 2024).

Por meio da decisão recorrida, no entanto, o juízo de primeiro grau entendeu que tal posicionamento violaria o direito à autodeterminação informacional e que configuraria tratamento discriminatório da pessoa em razão da deficiência.

O direito à autodeterminação informativa está ligado ao direito da reserva da intimidade e implica faculdade do indivíduo de dispor das informações pessoais e sua utilização por terceiros, conforme já destacado anteriormente neste trabalho.

Busca-se impedir que o indivíduo seja compreendido por meio de informações decorrentes de outra forma de comunicação. Para equacionar esta situação, pontua o acórdão que é necessário verificar qual tipo de dados será divulgado. Antes era necessário publicar o nome do requerido e o objeto da ação por meio de afixação de editais e publicação de anúncios. Com a reforma, não há previsão legal sobre itens obrigatoriamente publicizáveis, sendo que o juiz define o meio e o que será publicado.

Em Portugal, nos sites dos tribunais são disponibilizados, para acesso público, dados que identificam o autor e réu, o tribunal, o requerimento, o número do processo, o valor da ação e a espécie do processo. O sistema não impõe a divulgação dos fatos, encerrando o risco de divulgação de informações sobre a doença nos casos de acompanhamento.

No cenário anterior, em que existia a interdição e a inabilitação, a mera divulgação do tipo de ação por meio de anúncios e afixação de editais já revelava uma condição física ou comportamental relativa à pessoa.

Com a reforma, o art. 164, n. 2, “d” do CPC, previu para este tipo de ação a limitação de acesso aos autos<sup>61</sup>, diante da possibilidade da divulgação do conteúdo poder causar danos à intimidade e a dignidade.

O acórdão, em sua análise, tenta responder a seguinte pergunta: a informação que é divulgada no início e de acompanhamento processual faz com que a publicidade, que é obrigatória para o juiz, atinja o direito à autodeterminação informativa em qualquer caso?

O atingimento à autodeterminação informativa será maior ou menor a depender da ligação dos dados divulgados com os atributos da personalidade.

No caso em tela, os dados divulgados não são reveladores da condição médica, comportamental ou outra característica da individualidade pessoal ou social, ou seja, não são dados sensíveis.

Nestes casos, a publicização especial tem uma finalidade legítima, que seria dar a possibilidade a terceiros de terem ciência de que o possível sócio ou potencial contratante pode sofrer uma medida de acompanhamento com projeção em sua capacidade. Ademais, considerando a função da publicidade, esta se mostra proporcional para atingimento da tutela dos interesses patrimoniais de terceiros e do próprio acompanhado.

A inovação legislativa terminou por trazer uma restrição quanto à ocorrência de publicidade, quando demanda uma análise prévia pelo juiz acerca dos interesses quanto ao conteúdo, limitando os dados indispensáveis para dar conhecimento sobre a ação que pode interferir na validade de negócios; e quanto à forma, na medida em que excluiu a exigência de

---

<sup>61</sup> Sobre a possibilidade de restrição de acesso a informações processuais, pontua Teixeira (2019, p. 6-7): “Deste enquadramento decorre que não está em causa a legitimidade do acesso e tratamento de tais dados por parte do Tribunal, para a apreciação e decisão da causa, pois tal acesso não é sequer abrangido ou regulado pelo RGPD e o art. 9º reitera essa licitude. Cuida-se aqui apenas do acesso, da publicidade a terceiros que nada têm a ver com a causa e que não têm sequer que justificar a necessidade ou finalidade desse acesso. Nessas situações, consagra-se assim nas recentes alterações ao Código de Processo Civil supra referidas a possibilidade, e com ela a responsabilidade, de restringir a publicidade desses processos com fundamento no RGPD. A concreta forma de restrição dessa publicidade não está definida na lei nem em qualquer procedimento ou ferramenta informática, actualmente, cabendo assim a cada concreto Magistrado titular definir os moldes em que o desejar fazer ou considere adequado no processo. Tal poderá passar apenas por um despacho em que se determine as restrições à publicidade, total ou parcial ao processo, não cabendo naturalmente ao Juiz concretizar os termos técnicos em que tal despacho seja cumprido. Mas pode também passar pela utilização de ferramentas já existentes. Pense-se que num processo apenas constam dados sensíveis num ou outro documento e que o Magistrado titular pretende ele próprio determinar e controlar tal publicidade”.

publicação de editais e de anúncios em jornais de grande circulação sem impor nenhuma outra providência substitutiva.

Nesta linha, no novo sistema português, a restrição ao direito à intimidade decorrente da publicização destes casos é mais contida, em especial, se comparada ao sacrifício de não existir a divulgação. Isto porque o balanceamento entre a reserva da intimidade e o interesse de terceiros é feito perante o caso em concreto, sendo que a publicidade da ação ocorrerá sempre que for necessária.

Observa-se, nesta análise do precedente do Supremo Tribunal de Justiça de Portugal, que para conformar a aparente colisão entre a publicidade e a autodeterminação informativa<sup>62</sup>, foi levada em consideração o tipo dos dados compartilhados a depender da ligação dos dados com os atributos da personalidade.

Nesta constatação, foi levada em consideração a proporcionalidade entre a finalidade e o interesse público em tomar conhecimento dos referidos dados diante da autodeterminação, já que os dados divulgados seriam o mínimo necessário e não revelariam - na nova sistemática - a condição pessoal de saúde do titular dos dados, informação que seria sensível.

Como já destacado, no Brasil, são prestigiadas, com a decretação do sigilo, situações em que os dados e os atos processuais, ao serem divulgados, têm o potencial de causar prejuízo à intimidade e à privacidade do jurisdicionado - art. 189, inciso III do CPC -, como seria na hipótese de divulgação ampla e irrestrita de um relatório médico que revela uma moléstia grave.

Neste sentido, merece destaque a lei de n. 14.289, publicada em 3 de janeiro de 2022, e que tem impacto sobre este tema, pois disciplina a questão da obrigatoriedade da “preservação do sigilo quanto à condição de pessoa que vive com infecção pelos vírus da imunodeficiência

---

<sup>62</sup> Sobre a aparente colisão, no relatório da análise realizada sobre o tratamento de dados pessoais na consulta de jurisprudência, pontuou o CNJ (2021, p. 10) que: “No contexto da adequação dos serviços de divulgação de jurisprudência à LGPD, o grande desafio que se apresenta consiste em encontrar a justa medida, o ponto de equilíbrio entre dois valores constitucionais estruturantes: de um lado, o dever de publicização dos atos processuais, que viabiliza o controle social do Poder Judiciário e o próprio exercício de atividades jurídicas cotidianas, amplamente dependentes do conhecimento do conteúdo das decisões judiciais; de outro, o direito à proteção dos dados pessoais, em sua dimensão de “direito ao não conhecimento, tratamento, utilização e difusão de determinados dados pessoais pelo Estado ou por terceiros”. No enfrentamento desse desafio, deve-se evitar uma postura fatalista, que, es cuidando-se, de modo irrefletido, na tradição de publicidade processual e na primazia do interesse público, feche os olhos para os riscos gerados pela nova realidade tecnológica. Ao mesmo tempo, deve-se desviar de soluções simplistas, que ignorem as peculiaridades do tratamento de dados pessoais pelo Poder Público e desconheçam as dificuldades técnicas, administrativas e financeiras envolvidas na implementação de medidas proteção dos dados.”

humana (HIV) e das hepatites crônicas (HBV e HCV) e de pessoa com hanseníase e com tuberculose, nos casos que estabelece; e altera a Lei nº 6.259, de 30 de outubro de 1975”.

Neste sentido, dispõe a lei que:

Art. 1º Esta Lei dispõe sobre a obrigatoriedade de preservação do sigilo sobre a condição de pessoa que vive com infecção pelos vírus da imunodeficiência humana (HIV) e das hepatites crônicas (HBV e HCV) e de pessoa com hanseníase e com tuberculose, nos casos que estabelece.

Art. 2º É vedada a divulgação, pelos agentes públicos ou privados, de informações que permitam a identificação da condição de pessoa que vive com infecção pelos vírus da imunodeficiência humana (HIV) e das hepatites crônicas (HBV e HCV) e de pessoa com hanseníase e com tuberculose, nos seguintes âmbitos:

[...]

VI - processos judiciais;[...]

Art. 5º Nos inquéritos ou nos processos judiciais que tenham como parte pessoa que vive com infecção pelos vírus da imunodeficiência humana (HIV) e das hepatites crônicas (HBV e HCV) e pessoa com hanseníase e com tuberculose, devem ser providos os meios necessários para garantir o sigilo da informação sobre essa condição.

§ 1º Qualquer divulgação a respeito de fato objeto de investigação ou de julgamento não poderá fornecer informações que permitam a identificação de pessoa que vive com infecção pelos vírus da imunodeficiência humana (HIV) e das hepatites crônicas (HBV e HCV) e de pessoa com hanseníase e com tuberculose.

§ 2º Em julgamento que envolver pessoa que vive com infecção pelos vírus da imunodeficiência humana (HIV) e das hepatites crônicas (HBV e HCV) e pessoa com hanseníase e com tuberculose no qual não seja possível manter o sigilo sobre essa condição, o acesso às sessões somente será permitido às partes diretamente interessadas e aos respectivos advogados. [...].

Art. 6º O descumprimento das disposições desta Lei sujeita o agente público ou privado infrator às sanções previstas no art. 52 da Lei nº 13.709, de 14 de agosto de 2018, bem como às demais sanções administrativas cabíveis, e obriga-o a indenizar a vítima por danos materiais e morais, nos termos do art. 927 da Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil).

Parágrafo único. Nas situações em que for divulgada informação sobre a condição de pessoa que vive com infecção pelos vírus da imunodeficiência humana (HIV) e das hepatites crônicas (HBV e HCV) e de pessoa com hanseníase e com tuberculose por agentes que, por força de sua profissão ou do cargo que ocupam, estão obrigados à preservação do sigilo, e essa divulgação ficar caracterizada como intencional e com o intuito de causar dano ou ofensa, aplicar-se-ão em dobro:

I - as penas pecuniárias ou de suspensão de atividades previstas no art. 52 da Lei nº 13.709, de 14 de agosto de 2018;

II - as indenizações pelos danos morais causados à vítima (BRASIL, 2022).



Trata-se de lei recentemente promulgada, cuja constitucionalidade ainda não foi apreciada pelo Poder Judiciário, e que impõe um sigilo diferenciado sobre a condição de pessoa que vive com determinadas enfermidades.

Interessante observar que, embora a referida lei não trate da possibilidade de decretação de segredo de justiça nestas hipóteses, trata de restrição de acesso às sessões, o que denota o segredo.

Nestes casos, entende-se que o segredo de justiça deve ser decretado quando o sigilo sobre a condição pessoal não puder ser mantido, sempre que a preservação da intimidade o exigir, o que é o caso<sup>63</sup>.

Esta lei inova na medida em que determina que o descumprimento aos comandos ali previstos implicará sanções previstas no artigo 52, da Lei de n. 13.709, de 2018 (LGPD), “demais sanções administrativas cabíveis”, e indenizações por danos morais e materiais decorrentes do art. 927 do Código Civil.

O Poder Legislativo, sabedor da vulnerabilidade dos dados inseridos nos processos judiciais - mesmo que com a decretação do segredo de justiça -, pretende evitar que estas informações venham à tona a fim de evitar a sua propagação. Para atingir este objetivo, a lei prevê sanções de grande impacto pecuniário.

Trata-se de uma previsão normativa vigente, que determina sigilo de dado referente à condição de saúde de pessoa, que não poderá ser revelado em processo judicial, sob pena de aplicação de penalidade prevista na LGPD.

Com base no precedente português e no intuito de proteger os dados pessoais constantes nos processos judiciais, devem-se buscar parâmetros no sistema brasileiro de publicidade de

---

<sup>63</sup> Valendo-se mais uma vez do direito português, sobre a preocupação acerca dos dados de saúde, pontua Teixeira (2019, p. 6): “Os dados que revelem a origem racial ou étnica, opiniões políticas, convicções religiosas/filosóficas, filiação sindical, dados genéticos (ADN), dados biométricos, saúde, vida sexual ou orientação sexual são considerados no art. 9º do RGPD como dados especiais. É o caso, nomeadamente, dos dados de saúde. São inúmeros os casos de processo cíveis em que constam informações clínicas das partes ou de pessoas falecidas – pense-se em casos de ações declarativas para apreciação de responsabilidade civil por acidentes de viação ou de seguros de vida, em que tantas vezes se discute se uma doença era pré existente. A publicidade de tais processos, apesar de parecer clara nos termos dos n.ºs 1 e 2 do art. 163º, não parece ser compatível com o RGPD que, como decorre das alterações salientadas, tem agora também que ser considerado. Isto porque quanto aos dados sensíveis, o art. 9º do RGPD reduz significativamente os fundamentos de licitude para tratamento de dados especiais, consagrando como regra a proibição de tratamento”.

atos processuais que consideram a definição dos tipos de dados pessoais existentes nos atos processuais de forma que haja a disponibilização apenas das informações mínimas pessoais necessárias para a compreensão do processo.

### 3.5 DEFINIÇÃO DE PARÂMETROS GERAIS DE RESTRIÇÃO DE ACESSO A INFORMAÇÕES PROCESSUAIS PARA A PROTEÇÃO DE DADOS PESSOAIS

Como já tratado em tópicos anteriores, foi verificado que, com a publicização externa dos atos processuais, garante-se o direito à informação, desestimulando julgamentos arbitrários e possibilitando o controle dos atos judiciais por terceiros.

Dentre as hipóteses de controle, está a necessidade de identificação de litispendência, conexão, continência e coisa julgada, bem como de salvaguardar a força vinculante dos precedentes adotada pelo sistema jurídico nacional.

Sobre o atual panorama de amplo acesso a informações judiciais, Didier (2020, p. 138) destaca que:

Na atualidade, é possível obter amplo acesso a informações judiciais por meio de consultas a dados relativos a processos específicos nas páginas eletrônicas dos tribunais, pesquisas em bancos de dados de decisões judiciais e análise da publicação de atos de comunicação no Diário de Justiça Eletrônico. O alcance desses mecanismos é ainda mais acentuado com a adoção da interoperabilidade de sistemas processuais, da interface nacional única para os usuários externos, da utilização de API (Application Programming Interfaces) para aproveitamento das funcionalidades oferecidas por sistemas, da estruturação dos dados no maior nível possível de precisão e da disponibilização de arquivos em formato legível por máquina, características já previstas no art. 8º, parágrafo 3º, incisos I a VI, da Lei n. 12.527/2011 (Lei de Acesso à Informação), nos arts. 24, incisos VI e X, e 25, incisos I e III, da Lei n. 12.965/2014 (Marco Civil da Internet), no art. 29 da Lei n. 14.129/2021 (Lei do Governo Digital), bem como nas Resoluções n. 331/2020, 332/2020, 334/2020 e 358/2020 e na Recomendação n. 74/2020, todas do Conselho Nacional de Justiça.

Como a promulgação da LGPD, o Conselho Nacional de Justiça empregou todos os esforços para elaborar uma política de acesso às informações processuais.

Neste sentido, ponderam Oliveira e Silva (2023, p. 13):

E, posteriormente, em razão da promulgação da Lei n. 13.709/2018, que instituiu a Lei Geral de Proteção de Dados em nosso país, em 26 de abril de 2019, o CNJ, pela Portaria n. 63, instituiu um grupo de trabalho para elaborar estudos e propostas sobre a política de acesso às bases de dados dos processos judiciais dos Tribunais brasileiros, e especialmente o uso de tais informações para fins comerciais (art. 1º).

Paralelamente aos estudos elaborados realizados pelo grupo de trabalho, a Lawgorithm, uma associação de pesquisa em inteligência artificial e direito, fundada por professores das faculdades de direito, engenharia, matemática e filosofia da Universidade de São Paulo (USP), promoveu uma pesquisa com o objetivo de levantar informações sobre as práticas do mercado e dos órgãos públicos em relação ao acesso e tratamento de dados de processos perante o Poder Judiciário.

A Lawgorithm desenvolveu um estudo independente (Relatório de Acesso e Tratamento de Dados no Judiciário), que foi apresentado ao Grupo de Trabalho do CNJ.

No referido relatório, foram apresentadas as seguintes recomendações:

1. Dar continuidade à política de dados abertos para o Poder Judiciário, com expansão da digitalização e disponibilização ao público dos pronunciamentos judiciais e autos dos processos, como forma de propiciar o controle democrático das instituições e servidores que compõe o sistema judiciário e de estímulo ao mercado digital;
2. Aperfeiçoar o sistema de disponibilização de dados por meio do desenvolvimento de projeto próprio que propicie a interoperabilidade entre as diferentes plataformas digitais de tramitação de processos e uniformize a forma de identificação dos processos, formato de disponibilização (machinereadable format), bem como os metadados relevantes de modo a facilitar buscas e criar as bases para o desenvolvimento de ferramentas inteligentes que permitam acessar, analisar e comparar decisões judiciais;
3. Estimular a adoção de políticas de cache pelas organizações que usam dados judiciais, como forma de reduzir a demanda de acesso aos servidores;
4. Avaliar a adoção de uma API (application programming interface) para acesso a dados judiciais, que proporcionará conveniência às organizações que realizam processamento automatizado de dados e permitirá aos tribunais controlar o formato do acesso aos dados e a qualidade da informação fornecida ao público;
5. Avaliar a realização de projeto sobre anonimização de dados pessoais em pronunciamento judiciais e em documentos disponibilizados ao público, para conciliar o amplo acesso aos dados processuais com a proteção de dados pessoais;
6. Evitar a introdução de restrições ao acesso a documentos presentes nos autos do processo que possam limitar o controle democrático das instituições que compõem o sistema judicial, como a ocultação de nomes de magistrados e servidores que participam da elaboração dos pronunciamentos judiciais;
7. Empregar mecanismos que facilitem às partes a requisição de confidencialidade de documentos de natureza sigilosa; e 8. Difundir conhecimento a respeito das exigências postas pela Lei Geral de Proteção de Dados para o acesso a dados judiciais, bem como dos requisitos de segurança da informação a serem observados, em especial no que diz respeito a dados disponibilizados para o público.

A Recomendação n. 74 de 2020, que recomenda as medidas relacionadas à implementação da política de dados abertos no Poder Judiciário, foi então editada pelo

Conselho Nacional de Justiça e evidencia, em suas justificativas, a existência de “mercados digitais” que realizam tratamento de informações jurídicas:

CONSIDERANDO ser missão do Conselho Nacional de Justiça o desenvolvimento de políticas judiciárias que promovam efetividade e unidade do Poder Judiciário, orientadas para os valores de justiça e paz social;

CONSIDERANDO a publicidade dos atos processuais (art. 5º, LX, e no art. 93, IX, da Constituição da República Federativa do Brasil de 1988) e a transparência como princípios fundamentais para o controle democrático das atividades do Poder Judiciário;

CONSIDERANDO que o princípio de livre concorrência, consagrado no art. 170, IV, da Constituição da República Federativa do Brasil de 1988, impõe ao Estado a redução de barreiras ao livre desenvolvimento dos mercados digitais que processam e reutilizam informações jurídicas;

CONSIDERANDO o direito fundamental à proteção dos dados pessoais de jurisdicionados e demais sujeitos identificados ou identificáveis nos atos processuais; CONSIDERANDO a necessidade de proteger a personalidade e a autodeterminação informativa do indivíduo contra os riscos que podem decorrer do acesso massificado a informações contidas em processos judiciais;

CONSIDERANDO a edição da Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet);

CONSIDERANDO a crescente utilização da Internet e do emprego de modelos computacionais estruturados para o acesso e o processamento de dados disponibilizados pelos órgãos do Poder Judiciário;

CONSIDERANDO os benefícios do acesso ao conteúdo de pronunciamentos judiciais, em formato legível por máquina, para a difusão do conhecimento do Direito e contribuição à segurança jurídica;

CONSIDERANDO a importância do desenvolvimento da tecnologia, em particular de técnicas de inteligência artificial, para a sistematização e processamento de informações sobre a produção jurídica dos tribunais, como veículo para a promoção da cultura e da segurança jurídica;

CONSIDERANDO que a utilização de ferramentas como web scrapers para extração de conteúdo das plataformas de tribunais onera tanto o Poder Público quanto os agentes privados;

CONSIDERANDO os trabalhos desenvolvidos pelo Grupo de Trabalho instituído pela Portaria CNJ nº 63/2019, destinado ao exame da política de acesso às bases de dados processuais dos tribunais, especialmente quanto a sua utilização para fins comerciais;

CONSIDERANDO a decisão proferida pelo Plenário do Conselho Nacional de Justiça no julgamento do Procedimento de Ato Normativo nº 0007044-02.2020.2.00.0000, na 73ª Sessão Virtual, realizada no período de 1º a 9 de setembro de 2020; [...]. (BRASIL, 2020).

Neste sentido, a referida Recomendação estabelece:

Art. 1º Esta Recomendação estabelece diretrizes para avaliação e implementação de medidas destinadas à governança do acesso e uso massificado de dados no âmbito do Poder Judiciário, com exceção do Supremo Tribunal Federal.

Art. 2º Recomenda-se aos órgãos do Poder Judiciário a disponibilização ao público de APIs (Application Programming Interfaces) para que os dados existentes em seus sistemas de tramitação processual e repositórios de informações de processos e provimentos judiciais possam ser acessados em formato legível por máquina.

Parágrafo único. A disponibilização dos metadados dos processos judiciais constantes da Base Nacional de Dados do Poder Judiciário – DataJud, observará o disposto na Resolução CNJ nº 331/2020.

Art. 3º Os tribunais poderão avaliar a conveniência e oportunidade de cobrança pelo acesso massificado a dados.

§ 1º O valor da cobrança destina-se a suportar os custos de implantação e manutenção do sistema, devendo sua fixação ser efetuada na proporção do volume de dados utilizados.

§ 2º É assegurado acesso gratuito aos órgãos públicos e de pesquisa, estes definidos no art. 5º, XVIII, da Lei nº 13.709, de 14 de agosto de 2018.

Art. 4º Os tribunais deverão adotar medidas para a efetiva implementação das normas que dispõem sobre a uniformização dos identificadores e metadados armazenados que se referem aos pronunciamentos judiciais, a fim de racionalizar o acesso aos dados e criar condições para desenvolvimento de tecnologias que contribuam para o aperfeiçoamento do sistema jurisdicional.

Art. 5º Esta Recomendação entra em vigor na data da sua publicação (BRASIL, 2020).

Sobre esta recomendação, pontuam Olivera e Silva (2023, p. 15):

Após a conclusão dos trabalhos, o CNJ, no julgamento do Procedimento de Ato Normativo nº 0007044-02.2020.2.00.0000, na 73ª Sessão Virtual, realizada de 1º a 9 de setembro de 2020, editou recomendação estabelecendo diretrizes para avaliação e implementação de medidas destinadas à governança do acesso e uso massificado de dados no âmbito do Poder Judiciário, com exceção do Supremo Tribunal Federal.

No referido ato normativo, foi recomendada a disponibilização ao público de APIs (Application Programming Interfaces) para que os dados existentes em seus sistemas de tramitação processual e repositórios de informações de processos e provimentos judiciais possam ser acessados em formato legível por máquina, sendo que a disponibilização dos metadados dos processos judiciais constantes da Base Nacional de Dados do Poder Judiciário – DataJud, observará o disposto na Resolução CNJ nº 331, de 20 de agosto de 2020 (art. 2º).

Houve a previsão de que os Tribunais poderiam avaliar a conveniência e oportunidade de cobrança pelo acesso massificado a dados, sendo que o valor da cobrança seria destinado a suportar os custos de implantação e manutenção do sistema, devendo sua fixação ser efetuada na proporção do volume de dados utilizados (art. 3º).

Seria garantido o acesso gratuito aos órgãos públicos e de pesquisa, estes definidos no art. 5º, XVIII, da Lei n. 13.709, de 14 de agosto de 2018 (art. 3º, §2º).

Por fim, os Tribunais deveriam adotar medidas para a efetiva implementação das normas que dispõem sobre a uniformização dos identificadores e metadados armazenados que se referem aos pronunciamentos judiciais, a fim de racionalizar o acesso aos dados e criar condições para desenvolvimento de tecnologias que contribuam para o aperfeiçoamento do sistema jurisdicional (art. 4º).

Analisando as recomendações estabelecidas pelo CNJ, verificamos que somente foram acolhidas as sugestões de facilitação de acesso aos dados judiciais pelos entes privados, sendo que não houve nenhuma consideração quanto às medidas de proteção à privacidade das partes envolvidas no processo, tais como a adoção de medidas de anonimização e de facilitação de imposição de confidencialidade em documentos sigilosos.

Tal circunstância provoca grande preocupação, uma vez que o acesso irrestrito às informações das partes pode gerar graves danos à privacidade das partes, com violação à autodeterminação informativa e ao direito fundamental à proteção de dados, principalmente, em casos envolvendo conflitos trabalhistas, em que vários dados sensíveis são tratados e diante da possibilidade da formação de “listas sujas” para não contratação de empregados exerceram o seu direito constitucional de ação.

Mostra-se necessária, portanto, a efetiva proteção dos dados pessoais contidos nos processos judiciais, especialmente diante da existência de mecanismos tecnológicos avançados que são capazes de realizar o tratamento de dados, transformando informações que antes eram insignificantes em algo valioso, criando um verdadeiro perfil virtual da pessoa, passível de comercialização de diversas formas.

No caso analisado sobre o cruzamento de dados e tratamento pelos portais de buscas, foi possível notar que, sem interesse legítimo, há o tratamento de dados que propicia a informação sobre processos trabalhistas e criminais por mecanismos vedados pelo próprio sistema do Poder Judiciário, trazendo uma exposição excessiva.

Sobre o risco de exposição excessiva, no novo paradigma da economia digital, pondera Cueva (2020, p. 206):

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 os bens ou serviços que oferecem. Não é sem razão, assim, que vários sistemas judiciários, ao redor do mundo, impulsionados pelas leis de proteção de dados, já se têm preocupado em assegurar alguma opacidade aos dados pessoais públicos contidos nos autos de processos judiciais, para impedir o desvirtuamento da finalidade para a qual foram tratados.

Neste cenário, há um aparente conflito entre a publicidade e a privacidade e intimidade - que fundamentam a proteção de dados - que precisa ser equacionado. Sobre esta situação de conflito no âmbito público, destaca Wimmer (2021, p. 275):

A aparente tensão entre publicidade e privacidade tem sido ocasionalmente suscitada no contexto da necessidade de conciliar regras que impõem ao Estado um elevado grau de transparência quanto às suas atividades e aquelas que exigem que dados pessoais dos cidadãos sejam tratados de maneira a preservar a sua intimidade, vida privada, honra e imagem. Normas voltadas a ampliar a transparência do Estado –

como a Lei de Acesso à Informação (“LAI”) e as políticas de dados abertos – muitas vezes são construídos a partir de uma lógica de classificação das informações com base em seu grau de sigilo, que não necessariamente se alinha à lógica esposada por normas que tenham por objetivo a proteção de dados pessoais, como a LGPD. Enquanto a LGPD, por exemplo, utiliza a terminologia “dados pessoais” e define o princípio da transparência como “(...) a garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial”, a LAI utiliza o termo “informações pessoais” e insere o termo transparência no contexto do fomento a cultura de transparência na Administração Pública.

Considerando a forma como os dados são disponibilizados nos processos judiciais brasileiros na atualidade, é clara uma situação de colisão<sup>64 65</sup> entre o princípio da publicidade, os direitos fundamentais da proteção de dados, da autodeterminação informativa, da privacidade e da intimidade e as regras de acesso às informações processuais<sup>66</sup>.

Para equacionar tal situação é necessário traçar parâmetros que permitam a divulgação apenas das informações que sejam de interesse público e que tenham relação com a causa de pedir (o mínimo necessário) nos processos que não tramitem em segredo de justiça, limitando

---

<sup>64</sup> Sobre a questão da coexistência de princípios e regras, defende Ávila (2009, p. 120-121): “O modelo ora apresentado demonstra que um sistema não pode ser composto somente de princípios, ou só de regras. Um sistema só de princípios seria demasiado flexível, pela ausência de guias claros de comportamento, ocasionando problemas de coordenação, conhecimento, custos e controle de poder. E um sistema só de regras aplicadas de modo formalista seria demasiado rígido, pela ausência de válvulas de abertura para o amoldamento das soluções às particularidades dos casos concretos. Com isso se quer apenas dizer que, a rigor, não se pode dizer nem que os princípios são mais importantes do que as regras, nem que as regras são mais necessárias que os princípios. Cada espécie normativa desempenha funções diferentes e complementares, não se podendo sequer conceber uma sem a outra, e outra sem a uma. Tal observação é da mais alta relevância, notadamente tendo em vista o fato de que a Constituição Brasileira é repleta de regras, especialmente de competência, cuja finalidade é, precisamente, alocar e limitar o exercício de poder”.

<sup>65</sup> Ainda sobre os princípios e regras, entende Canotilho (2006, p. 358-359): “Com esta diferença: enquanto a teoria dos direitos como princípios ergue a ponderação a esquema metódico básico, pois os princípios “pesam-se” sem recorrer à lógica do “tudo ou nada”, ou “de ou um ou outro”, de “direito superior-direito inferior”, as regras reclamam em toda a sua radicalidade aplicação ou não aplicação. Mas, o que vale a dogmática civilística insistir na ideia fixa de regras quando os direitos de personalidade são “pesados” e “ponderados” no uso de conflito com outros direitos? A maior racionalidade da metódica aplicativa das *regras*, que, por vezes, também é invocada, não conduz como se vê, a soluções muito diferentes, podendo talvez invocar que o recorte mais fino dos pressupostos de facto e de direito tornará a fundamentação de restrições e os resultados obtidos mais previsível, embora não necessariamente mais justa”.

<sup>66</sup> Sobre a relação entre a publicidade e a LGPD, entendem Bulzico e Sousa (2022, fls. 155): “Tem sido intensa a discussão acerca de suposta incompatibilidade entre a nova Lei de proteção de dados e o Princípio Constitucional da Publicidade dos Atos Processuais. Contudo, tal discussão, conforme se verifica da leitura do presente trabalho, não merece prosperar, ou mesmo ser tomada como ponto crucial na discussão que envolve a temática da proteção de dados. Isso se dá pelo fato de que tais princípios — publicidade dos atos processuais e proteção dos dados pessoais — sempre coexistiram de forma pacífica e complementar, não havendo do que se falar em incompatibilidade e divergência entre estes, muito pelo contrário, importa destacar que a LGPD surge como ferramenta necessária a evolução e dinamização do princípio da publicidade processual”.

o acesso a informações que não sejam de interesse público e de caráter sensível e ou íntimo, no intuito de salvaguardar os direitos fundamentais acima elencados.

Esta limitação de acesso às informações pessoais, que consideraria o tipo de dado pessoal, compreenderia tanto às informações que são disponibilizadas por meio de publicações, como também aquelas que são obtidas por meio do acesso aos autos dos processos, de modo que não violaria a garantia constitucional à publicidade, que é vinculada aos atos processuais.

Para esta proposta, que visa readequar o sistema de publicidade dos atos processuais a esta nova demanda social de proteção de dados num ambiente de avanço tecnológico sem precedentes, parte-se dos seguintes pressupostos: (i) em regra, não pode existir limitação de acesso de informação entre as partes e demais sujeitos do processo, sendo que eles têm o dever de salvaguardar os dados que tiveram acesso por conta da demanda, evitando o compartilhamento com terceiros; (ii) os processos em segredo de justiça são sigilosos, em que há adoção de técnicas de pseudoanonimização para publicidade externa e restrição de acesso público a documentos processuais; (iii) o acesso público aos autos processuais está condicionado a não violação da privacidade e da intimidade; (iv) os processos que não estão em segredo de justiça demandam a criação de mecanismos de limitação<sup>67</sup> de acessos a dados pessoais; (v) os advogados têm amplo acesso aos autos que não tramitam em segredo de justiça, devendo zelar pelas informações que obtêm em decorrência deste acesso; e (vi) o Estado, por meio do Poder Judiciário, é quem deve garantir a proteção dos dados pessoais contidos no processo, limitando o acesso a informações de seus servidores ao mínimo necessário para o desempenho de suas funções, porque é o responsável pela gestão do sistema dos processos digitais e porque detém tecnologia para tanto.

Dentro da classificação proposta em tópico antecedente, em que se separa os dados pessoais contidos em um processo judicial em três tipos, dados pessoais não relacionados à

---

<sup>67</sup> Sobre a limitação dos dados pessoais contidos nos processos judiciais em outros países, explica Cueva (2020, p. 208-209) que: “Outros países europeus também têm se adaptado ao novo regime de proteção de dados pessoais. A Corte de Cassação da França, por exemplo, desde 2016 já conta com um software para efetuar a anonimização de suas decisões. O Judiciário da Inglaterra já tem, desde maio de 2018, um órgão encarregado de processar as reclamações relativas ao tratamento de dados pessoais pelos tribunais, magistrados e servidores da justiça ingleses. Na Espanha, o Conselho Geral do Poder Judiciário tem um delegado de proteção de dados pessoais e disponibiliza em seu sítio na internet um minudente registro de atividades de tratamento, com descrição, para cada uma das atividades, da finalidade do tratamento, de sua base jurídica, das categorias de dados e de destinatários atingidos, do prazo de conservação e das medidas de segurança requeridas, entre outras informações úteis para que se proceda ao tratamento de dados pessoais no âmbito dos tribunais de forma segura e em conformidade com a lei nacional e com o RGPD”.



causa de pedir, dados pessoais relacionados à causa de pedir e dados pessoais sensíveis e íntimos, propõe-se que sejam criadas restrições de acesso aos: (i) dados pessoais não relacionados à causa de pedir, por não terem relevância e nem interesse público em razão do seu conteúdo privado, devendo ser destacados e inseridos em um sistema para acesso exclusivo de juízes e sujeitos envolvidos na demanda, mediante a indicação direta pelo próprio interessado em proteger os dados; (ii) dados pessoais sensíveis e íntimos, que não tiverem relação com a causa, que também deverão ser objeto do sistema seletivo de restrição proposto no item (i); (iii) dados pessoais sensíveis e íntimos que tenham referência indispensável na causa de pedir, devendo ser decretado o segredo de justiça<sup>68</sup> para preservar a intimidade, com base no inciso III, do artigo 189, do Código de Processo Civil.

A proposta envolve, basicamente, a instituição de um sigilo extraprocessual e seletivo de dados pessoais que não têm interesse público e a decretação de segredo de justiça em processos cuja causa de pedir envolva dados sensíveis e íntimos. Os demais dados, de interesse público, não sofreriam limitações de acesso, sendo o mínimo necessário para a compreensão da lide e o exercício do controle já apontado no Estado Democrático de Direito.

O Enunciado 681, do Conselho da Justiça Federal, ao tratar de documentos em que há dados pessoais sensíveis, entende que:

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.

Tal previsão, no entanto, não atende a hipótese de proteção quando o dado sensível integra a causa de pedir da ação, o que – no entender desta proposta – importaria a decretação do segredo de justiça.

---

<sup>68</sup> No relatório da análise realizada sobre o tratamento de dados pessoais na consulta de jurisprudência, pontuou o CNJ (2021, p. 15) que: “Para tornar efetiva a proteção dos dados pessoais nas hipóteses em que não bastarem a simples omissão ou a mera pseudonimização das informações nos textos judiciais, os(as) magistrados(as) podem recorrer ao instituto do segredo de justiça. (...) Por fim, a legislação brasileira tipifica como crime, punido com pena de reclusão de dois a quatro anos e multa, a conduta de “quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei” (art. 10 da Lei n.º 9.296, de 1996). A decretação do segredo de justiça, portanto, tem o condão de ativar algumas camadas adicionais de proteção aos dados pessoais, razão pela qual devem os(as) magistrados(as) considerar detidamente a possibilidade de acionar esse instituto jurídico, inclusive de ofício, sempre que a exposição das informações processuais gerar risco desmesurado à privacidade dos cidadãos”.

Esta proposta leva em consideração a natureza das informações e a sua importância, atendendo ao que preza a LGPD.

Visa-se, com esta proposta, suprir uma demanda de definição de regras sobre quais dados devem estar em sigilo<sup>69</sup> nos atos processuais diante do recorte apresentado.

Desta forma, estariam protegidos os dados pessoais que não têm interesse público, os dados sensíveis e íntimos, e seria garantida a publicidade dos dados pessoais dentro do mínimo necessário para compreensão da lide, permitindo o monitoramento da aplicação dos institutos processuais.

Ademais, num sistema processual em que se emprega a força vinculante dos precedentes, a publicidade dos atos processuais é indispensável para o cotejo fático e jurídico do precedente com o caso que está em análise, sendo dispensável, na maior parte dos casos, o acesso a maior parte dos dados pessoais disponíveis no processo para atingimento desta finalidade.

Partindo dos parâmetros sugeridos, o Conselho Nacional de Justiça pode buscar o diálogo com os tribunais brasileiros no intuito de definir o melhor formato a ser aplicado no país, preferencialmente de forma padronizada, no intuito de implementar uma política eficiente e eficaz de proteção dos dados pessoais contidos nos processos judiciais.<sup>70</sup>

Sobre as ações a serem adotadas pelo Conselho Nacional de Justiça em relação à proteção de dados pessoais contidos nos processos judiciais, Cueva (2020, p. 208-209) aponta que:

---

<sup>69</sup> Acerca da definição de dados sigilosos, sugere Cardoso (2021, p. 2) que: “Como não existem na LGPD e no CPC regras específicas sobre a definição de todos os dados pessoais que devem ser considerados sigilosos nos atos processuais, a sua definição deverá ocorrer na prática das decisões judiciais e na regulamentação da aplicação da Lei Geral de Proteção de Dados pelo Judiciário”.

<sup>70</sup> No mesmo sentido, pondera Zanetti (2021): “Por fim, visando trazer algum contributo minimamente propositivo à presente discussão, acredita este autor que um primeiro passo importante para a melhor acomodação da problemática seria a celebração de um Acordo de Cooperação Técnica entre a Autoridade Nacional de Proteção de Dados (ANPD) e o Conselho Nacional de Justiça (CNJ) 11. Neste sentido, em comentários ao art. 194, do Código de Processo Civil, Nelson Nery Jr. e Rosa Maria de Andrade Nery recomendam que ‘(...) cada Tribunal deverá ter o cuidado de não expor informações desnecessárias e que possam comprometer/constranger a pessoa, mesmo que o processo não siga em segredo de justiça’. Tal orientação corrobora a presente conclusão, uma vez que permitiria, que as autoridades competentes, em ambiente apropriado, melhor estabeleçam o referido diálogo das fontes entre CPC e LGPD na rotina dos Tribunais pátrios, dando maior efetividade ao disposto no art. 194, do CPC13, sobretudo no que concerne a mecanismos de pseudonimização de dados pessoais veiculados em processos e peças processuais, de modo a limitar o acesso de terceiros (ou seja, atores externos à relação inter partes) quanto a dados pessoais, especialmente aqueles considerados sensíveis, nos termos do art. 5º, II, da LGPD”.

Caberá ao Conselho Nacional de Justiça iniciar um diálogo estruturado com os tribunais para definir em conjunto as balizas que deverão orientar a observância da LGPD, por meio de rotinas e práticas que assegurem a publicidade dos atos e documentos processuais, sem ameaça aos direitos fundamentais à privacidade e à intimidade dos jurisdicionados e de terceiros. É possível imaginar, ainda, que o legislador venha a se defrontar com a necessidade de anonimizar alguns dados pessoais contidos em processos ou decisões judiciais, a exemplo do que já se verifica em outras jurisdições, para evitar a formação, dissociada da finalidade do tratamento originários dos dados, de perfis informacionais de jurisdicionados e de terceiros.

Uma vez adotados estes parâmetros, é fundamental que seja fiscalizada a sua implementação, pois o que se vê, atualmente, é que nem mesmo nos processos que tramitam em segredo de justiça os tribunais têm conseguido que as publicações sejam anonimizadas para restringir o acesso a informações pessoais.

Até mesmo porque, no caso de um indevido tratamento de dados pessoais por terceiros, que somente foram disponibilizados em um determinado processo judicial, o caminho possível seria o de buscar os registros de acesso aos autos - regulamentado no parágrafo segundo do art. 3º da Resolução 121 do CNJ - para se tentar buscar a origem da ocorrência.

No entanto, como visto por meio do caso ARE 1307386, ainda pendente de julgamento perante o Supremo Tribunal Federal, os tratamentos poderão decorrer de sistemas automatizados de empresas com finalidades comerciais, que não ficam registrados.

### 3.6 A IMPORTÂNCIA DA IMPLANTAÇÃO E EXECUÇÃO DE UM PROGRAMA DE COMPLIANCE

Sobre a natureza da relação entre o Poder Público e o cidadão, esclarece Wimmer (2021, p. 286):

A relação entre o Poder Público e cidadão não é facultativa. Ela se inicia no dia do nascimento de cada indivíduo e perdura até mesmo após sua morte, fazendo-se presente em quase todas as dimensões da vida humana. A compreensão do caráter contínuo, e não episódico, de tal relação conduz, necessariamente, ao entendimento de que a confiança de parte a parte deve ser conquistada e mantida continuamente, não se esgotando na simples existência de uma base legal para o tratamento de dados. A construção de uma relação de confiança entre Estado e cidadãos requer a clara percepção da responsabilidade do Estado de, com transparência e accountability, tratar e custodiar dados de seus cidadãos tendo em vista a sua proteção e o atingimento

do interesse público em sua acepção mais ampla, considerado seu compromisso com a democracia e com a concretização de direitos fundamentais.

Esta relação entre o Poder Público e o cidadão está mais do que presente no serviço prestado pelo Poder Judiciário.

Nesta linha, diante da proposta sugerida no tópico anterior, é necessária a implantação de um programa pleno de *compliance* – ainda não tão comum no setor público - para evitar<sup>71</sup> incidentes de vazamento de dados<sup>72</sup> e garantir a execução da sugestão proposta.

Sobre os desafios decorrentes do advento da LGPD e a necessidade de implantação do *compliance* digital pelo Poder Judiciário Brasileiro, destaca Santos (2021, p. 92):

O advento da Lei Geral de Proteção de Dados Pessoais, Lei n.º 13.709, de 14 de agosto de 2018 e suas posteriores alterações, fez aumentar a complexidade da proteção aos dados dos jurisdicionados, bem como dos servidores e juízes vinculados aos tribunais brasileiros. Essa nova legislação, baseada em grande parte no Regulamento Geral sobre a Proteção de Dados existente na Europa, apresenta uma série de desafios ao Poder Judiciário brasileiro, pois as adequações, reorganizações e mudanças na cultura da proteção de dados, assim como a implantação ou ampliação do *compliance* digital, com a finalidade de proteger de vazamentos e má utilização, os dados presentes em seus sistemas e convênios, confiados a esse Poder Estatal de boa-fé e com a confiança de que serão preservados e bem geridos, estando a personalidade e a dignidade de quem integra uma lide protegidas de investidas de hackers ou pessoas e entidade que possam, de alguma forma, lucrar com a comercialização desses dados, ou até mesmo infligir algum dano, seja moral ou material ao usuário do sistema.

Ademais, sobre o programa de *compliance*, Dias explica que (2019, p. 57):

[...] programa de *compliance* pode ser compreendido como um conjunto sistemático de esforços realizados por integrantes da pessoa jurídica com objetivo de assegurar que as atividades empreendidas pelo ente se darão em absoluta correção, não violando a legislação concernente a tais atividades. No entanto, salienta que o sistema de comprometimento ou cumprimento normativo deve ser pensado levando em consideração a legislação e os riscos específicos. O programa de *compliance* deve ser

---

<sup>71</sup> Doneda e Machado pontuam que (2021, p. 344-345): “[...] é necessária uma preocupação com a segurança da informação para bancos de dados que possuem não só dados sensíveis ou sigilosos, mas também dados cadastrais. Deve-se afastar a ideia de que o tratamento de dados cadastrais é livre de riscos para o sujeito”.

<sup>72</sup> Segundo Wimmer (2021, p. 285): “A LGPD atribuiu a autoridade nacional o papel de elaboração de informe com medidas cabíveis para fazer cessar a violação (art. 31) e previu a possibilidade de aplicação, a órgãos e entidades públicas, das sanções de advertência, publicização da infração, bloqueio e eliminação dos dados pessoais a que se refere a infração. Importa notar que a sanção de multa prevista na LGPD claramente não é aplicável ao Poder Público, mas que multas previstas em outras normas aplicáveis ao Estado poderão incidir sobre órgãos e entidades no setor público, no contexto de ações de controle e fiscalização”.

adequado, entre outros, às características, especificidades, estrutura, setores de atuação, riscos legais e regulatórios a que exposta a organização. Deve ter o comprometimento de todos e ser desenvolvido sob medida para a empresa. [...]

Assim, a efetividade de um programa de cumprimento normativo associa-se à prevenção da ocorrência de violações legais - reduzindo o risco de sanções diversas por descumprimento normativo e de exposição negativa da organização perante a sociedade - ao tempo em que por antecedência lógica, permite aos administradores conhecer e corrigir as distorções e violações detectadas, bem como identificar responsabilidades. No entanto, seu principal objetivo deve ser promover uma cultura que observe as normas e os valores da sociedade.

Sobre a eficácia e a eficiência na execução de práticas administrativas, esclarecem Souza e Faria (2017, p. 279):

[...] compete ao Estado introduzir ações inovadoras para assegurar boa gestão. Para tanto, seu perfil deve ser de Estado “inteligente-mediador-indutor”, com instituições democráticas sólidas, norteadas pela eficiência, eficácia e efetividade, competência dos recursos humanos, dentre outros.

[...] Muito se tem discutido sobre a influência da eficácia e da eficiência nos mecanismos de gestão pública, haja vista que as investigações sobre qualquer atuar falho da Administração Pública levam a conclusões de que a atuação gerencial foi deficiente. Daí se pensar que quanto melhor eficácia e eficiência na execução das práticas administrativas, melhor gestão e controle das atividades envolvidas, sejam elas de cunho econômico, sejam propriamente de cunho administrativo.

Sobre a questão da proteção de dados no setor público, pontua Wimmer (2021, p. 274-275):

O desafio de interpretação a aplicação da legislação de proteção de dados pessoais ao setor público é significativo, e deve partir do reconhecimento das tensões e dualidades anteriormente exploradas. Se a motivação e a legitimidade do governo ao tratar dados pessoais devem necessariamente ser compreendidas como distintas daquela dos agentes privados, sua responsabilidade é, também, maior, dado que eventual mau uso de dados pelo Estado produz impactos abrangentes não apenas sobre a esfera de direitos individuais, mas sobre a sociedade como um todo. É por essa razão que os mais importantes instrumentos internacionais de proteção de dados indicam que os princípios e regras referentes à proteção de dados pessoais se aplicam tanto ao setor público como ao setor privado.

Especificadamente em relação à gestão do sistema judicial, Sousa Santos (2005, p. 90), ao falar sobre as novas tecnologias de comunicação e de informação (NTCI), destaca:

No que respeita à democratização do acesso ao direito e à justiça, as novas tecnologias de informação possibilitam mais circulação de mais informação e, portanto, um direito e uma justiça mais próximos e mais transparentes. Por exemplo, facilitam o acesso a bases de dados jurídicos, a informações fundamentais para o exercício de direitos, e possibilitam o exercício fácil de um conjunto de direitos e de deveres dos cidadãos.

No entanto, mais adiante, pontua Sousa Santos que (2005, p. 105), que, em relação ao impacto da tecnologia de comunicação e de informação na gestão do sistema judiciário, existem oportunidade para melhorar a eficácia e a administração dos tribunais.

Neste cenário, em que pese os avanços tecnológicos impliquem a necessidade de uma atenção maior em relação à proteção dos dados processuais, estes também propiciam oportunidades para melhorar a eficácia e racionalizar a gestão nos tribunais.

Afinal, novos sistemas são criados, com ferramentas de controle mais precisas e que podem auxiliar no monitoramento dos processos de gestão.

A proposta de limitação de acesso a dados processuais, na forma sugerida no tópico anterior, demandará cuidados de execução e fiscalização.

Pretende-se, com esta proposta, que seja garantida a publicidade dos dados processuais, bem como que sejam garantidos os direitos à privacidade, à intimidade e à autodeterminação informativa, com a divulgação do mínimo necessário para a compreensão da lide.

## CONCLUSÃO

A publicidade dos atos processuais é uma garantia processual concedida às partes, que prestigia o direito à informação, possibilitando o controle dos atos judiciais por terceiros e desestimulando julgamentos arbitrários. Trata-se, assim, de um princípio fundamental para a sustentação do Estado Democrática de Direito.

O ordenamento jurídico brasileiro já prevê hipóteses em que a publicidade é relativizada, visando à defesa da privacidade ou quando o interesse social assim o exigir, com a imposição do sigilo e a decretação do segredo de justiça.

Ademais, a Lei n. 13.709/2018, conhecida como a Lei Geral de Proteção de Dados (LGPD), que disciplina a proteção de dados no Brasil, salvaguarda os dados pessoais e elenca o respeito à privacidade, a inviolabilidade da intimidade e à autodeterminação informativa como fundamentos para a proteção de dados pessoais.

Diante da institucionalização do processo eletrônico no país e da ausência de normas efetivas que garantam a restrição de acesso a dados que não tenham interesse público, os dados pessoais constantes nos processos estão expostos e vulneráveis a um tratamento ilegítimo, conforme revela o tema 1141 do Supremo Tribunal Federal.

Os dados inseridos nos processos estão efetivamente em situação de vulnerabilidade diante do avanço da tecnologia que viabilizou a criação de *softwares* capazes de obter e processar os dados encontrados nos processos judiciais. A situação é mais grave porque foi constatado que, em um processo judicial, é possível acessar uma série de dados pessoais, inclusive dados sensíveis, das partes envolvidas.

A publicação da Lei 14.289/2022, que torna obrigatório o sigilo “sobre a condição de pessoa que vive com infecção pelos vírus da imunodeficiência humana (HIV) e das hepatites crônicas (HBV e HCV) e de pessoa com hanseníase e com tuberculose”, inclusive em processos judiciais, revela, justamente, a preocupação do Poder Legislativo em relação à disponibilização e acesso de dados pessoais sensíveis em processos judiciais.

No cenário atual, não há hipótese legalmente instituída para se garantir um sigilo seletivo e a não propagação dos dados pessoais que não sejam de interesse público.

Após a análise da extensão atual dos direitos fundamentais à privacidade, à intimidade, à autodeterminação informativa e à proteção de dados, mostrou-se necessária a limitação de acesso às informações constantes em atos processuais para a preservação dos dados pessoais, sem que se viole a garantia constitucional à publicidade para o convívio pleno entre os princípios e regras vigentes.

O presente trabalho evidenciou que é possível a limitação de acesso às informações constantes em atos processuais para a preservação dos dados pessoais em nome do livre desenvolvimento da personalidade, sem que se viole a garantia constitucional à publicidade.

Neste sentido, foram definidos parâmetros gerais de restrição de acesso a informações processuais para proteção de dados pessoais, tendo partido dos seguintes pressupostos: (i) em regra, não pode existir limitação de acesso de informação entre as partes e demais sujeitos do processo, sendo que eles têm o dever de salvaguardar os dados que tiveram acesso por conta da demanda, evitando o compartilhamento com terceiros; (ii) os processos em segredo de justiça são sigilosos, em que há adoção de técnicas de pseudoanonimização para publicidade externa e restrição de acesso público a documentos processuais; (iii) o acesso público aos autos processuais está condicionado a não violação da privacidade e da intimidade; (iv) os processos que não estão em segredo de justiça demandam a criação de mecanismos de limitação<sup>73</sup> de acessos a dados pessoais; (v) os advogados têm amplo acesso aos autos que não tramitam em segredo de justiça, devendo zelar pelas informações que obtêm em decorrência deste acesso; e (vi) o Estado, por meio do Poder Judiciário, é quem deve garantir a proteção dos dados pessoais contidos no processo, limitando o acesso a informações de seus servidores ao mínimo

---

<sup>73</sup> Sobre a limitação dos dados pessoais contidos nos processos judiciais em outros países, explica Cueva (2020, p. 208-209) que: “Outros países europeus também têm se adaptado ao novo regime de proteção de dados pessoais. A Corte de Cassação da França, por exemplo, desde 2016 já conta com um software para efetuar a anonimização de suas decisões. O Judiciário da Inglaterra já tem, desde maio de 2018, um órgão encarregado de processar as reclamações relativas ao tratamento de dados pessoais pelos tribunais, magistrados e servidores da justiça ingleses. Na Espanha, o Conselho Geral do Poder Judiciário tem um delegado de proteção de dados pessoais e disponibiliza em seu sítio na internet um minudente registro de atividades de tratamento, com descrição, para cada uma das atividades, da finalidade do tratamento, de sua base jurídica, das categorias de dados e de destinatários atingidos, do prazo de conservação e das medidas de segurança requeridas, entre outras informações úteis para que se proceda ao tratamento de dados pessoais no âmbito dos tribunais de forma segura e em conformidade com a lei nacional e com o RGPD”.



necessário para o desempenho de suas funções, porque é o responsável pela gestão do sistema dos processos digitais e porque detém tecnologia para tanto.

Para tanto, foram classificados os dados pessoais contidos em um processo judicial em três tipos, quais sejam, dados pessoais não relacionados à causa de pedir, dados pessoais relacionados à causa de pedir e dados pessoais sensíveis e íntimos.

Nesta linha, foi proposta a restrição de acesso aos seguintes dados: (i) dados pessoais não relacionados à causa de pedir, por não terem relevância e nem interesse público em razão do seu conteúdo privado, devendo ser destacados e inseridos em um sistema para acesso exclusivo de juízes e sujeitos envolvidos na demanda, mediante a indicação direta pelo próprio interessado em proteger os dados; (ii) dados pessoais sensíveis e íntimos, que não tiverem relação com à causa de pedir, que também deverão ser objeto do sistema seletivo de restrição proposto no item (i); (iii) dados pessoais sensíveis e íntimos que tenham referência indispensável na causa de pedir, devendo ser decretado o segredo de justiça para preservar a intimidade, com base no inciso III do artigo 189, do Código de Processo Civil.

Trata-se da instituição de um sigilo seletivo e extraprocessual de dados pessoais, que não têm interesse público, e a decretação de segredo de justiça em processos cuja causa de pedir envolva dados sensíveis e íntimos. Os demais dados, de interesse público, não sofreriam limitações de acesso, sendo o mínimo necessário para a compreensão da lide e o exercício do controle já apontado no Estado Democrático de Direito.

Com a adoção das medidas sugeridas, por meio de soluções a serem implementadas pelo Conselho Nacional de Justiça (CNJ), em conjunto com os tribunais brasileiros e com a Autoridade Nacional de Proteção de Dados, faz-se necessária a adoção de medidas para evitar inconsistências, inclusive, no que se referem a um programa de *compliance*.

## REFERÊNCIAS

- ABDO, Helena. A garantia da publicidade do processo e a divulgação de atos processuais pela mídia: limites e precauções atinentes ao processo civil. *In: COMPEDI, Anais...* Disponível em: < [http://www.conpedi.org.br/manaus/arquivos/anais/salvador/helena\\_najjar\\_abdo.pdf](http://www.conpedi.org.br/manaus/arquivos/anais/salvador/helena_najjar_abdo.pdf)>. Acesso em: 11 de jan. de 2021.
- ALEXY, Robert. *Teoria dos direitos fundamentais*. Tradução de Virgílio Afonso da Silva. São Paulo: Malheiros Editores, 2008.
- ALMONDI, Veridiana. Autodeterminação informacional na LGPD: antecedentes, influências e desafios. *In: CUEVA, Ricardo Villas Bôas; DONEDA, Danilo; MENDES, Laura Schertel (Org.). Lei Geral de Proteção de Dados (Lei n. 13.709/2018). A caminho da efetividade: contribuições para a implementação da LGPD*. São Paulo: Thomson Reuters Brasil, 2020, p. 177-192.
- ANDRADE, Rafael Campedelli; MARANHÃO, Juliano. O desafio da harmonização entre publicidade e proteção de dados pessoais. *Revista Consultor Jurídico*, 2 fev. 2021. Disponível em: <<https://www.conjur.com.br/2021-fev-02/direito-digital-harmonizacao-entre-publicidade-protecao-dados-pessoais>>. Acesso em: 4 jan. 2022.
- ARANHA, Estela; FERREIRA, Maria Lucia. O Direito Fundamental à Proteção de Dados e a importância da emenda constitucional n 17/2019. *OAB-RJ*, 27 jan. 2020. Disponível em: <https://www.oabRJ.org.br/noticias/artigo-direito-fundamental-protecao-dados-importancia-proposta-alteracao-constitucional>. Acesso em: 12 jan. 2023.
- ÁVILA, Humberto. *Teoria dos Princípios*. Da definição à aplicação dos princípios jurídicos. São Paulo: Malheiros Editores, 2009.
- BARROS, Renato da Costa Lino de Goes. *A publicidade do processo e a preservação dos direitos fundamentais à proteção de dados e à privacidade: Limites para salvaguarda dos dados pessoais no processo judicial sob a luz da constituição federal e dos preceitos da lei geral de proteção de dados*. Anteprojeto de pesquisa apresentado no processo seletivo do Programa de Doutorado do Instituto Brasiliense de Direito Público. Brasília, jan. 2021.
- BARROS, Renato; BRANCO, Mauricio de Melo Teixeira; PAMPLONA FILHO, Rodolfo Mário Veiga. Fundamentação Material dos Direitos Fundamentais na Contemporaneidade. *Revista Trimestral de Direito Civil*, v. 45, p. 63-90, 2010.
- BETTI, Emilio. *Interpretação da Lei e dos Atos Jurídicos*. São Paulo: Martins Fontes. 2007
- BEZERRA, Arthur Coelho. Vigilância e cultura algorítmica no novo regime global de mediação da informação. *Perspect. ciênc. inf.*, Belo Horizonte, v. 22, n. 4, p. 68-81, dez. 2017. Disponível em: <[http://www.scielo.br/scielo.php?script=sci\\_arttext&pid=S1413-99362017000400068&lng=en&nrm=iso](http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1413-99362017000400068&lng=en&nrm=iso)>. Acesso em: 10 jan. 2021.

BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado. *In*: CUEVA, Ricardo Villas Bôas; DONEDA, Danilo; MENDES, Laura Schertel (Org.). *Lei Geral de Proteção de Dados (Lei n. 13.709/2018)*. A caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020, p. 39-54.

BOAVENTURA, Edivaldo M. *Metodologia da pesquisa*: monografia, dissertação e tese. São Paulo: Atlas, 2004.

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/LEIS/L8080.htm](https://www.planalto.gov.br/ccivil_03/LEIS/L8080.htm)>. Acesso em: 2 jan. 2021.

\_\_\_\_\_. Conselho Nacional de Justiça. *Pedido de Providências n. 0003869-39.2016.2.00.0000*. Relator: Ministro Luciano Frota. Data de julgamento: 6 de março de 2018. Disponível em: [www.cnj.jus.br](http://www.cnj.jus.br). Acesso em: 15 abr. 2024.

\_\_\_\_\_. Conselho Nacional de Justiça. *Resolução n. 121 de 5 de outubro de 2010*. Dispõe sobre a divulgação de dados processuais eletrônicos na rede mundial de computadores, expedição de certidões judiciais e dá outras providências. Disponível em <https://www.cnj.jus.br>. Acesso em: 30 mar. 2024.

\_\_\_\_\_. Conselho Nacional de Justiça. *Resolução n. 137 de 13 de julho de 2011*. Regulamenta o banco de dados de mandados de prisão, nos termos do art. 289-A do CPP, acrescentado pela Lei n. 12.403, de 4 de maio de 2011, e dá outras providências. Disponível em: <[https://www.tjsp.jus.br/Download/SPI/Downloads/ManualBNMP\\_VRS8.pdf](https://www.tjsp.jus.br/Download/SPI/Downloads/ManualBNMP_VRS8.pdf)>. Acesso em: 30 mar. 2024.

\_\_\_\_\_. Conselho Nacional de Justiça. *Resolução n. 143 de 25 de abril de 2023*. Regulamenta a estrutura, a geração e a validação do Código Nacional de Matrícula – CNM, dispõe sobre a escrituração da matrícula no registro de imóveis, e dá outras providências. Disponível em: <<https://atos.cnj.jus.br/files/original15183420230426644940cabe4c2.pdf>>. Acesso em: 30 mar. 2024.

\_\_\_\_\_. Conselho Nacional de Justiça. *Resolução n. 345 de 9 de outubro de 2020*. Dispõe sobre o “Juízo 100% Digital e dá outras providências”. Disponível em: <https://www.cnj.jus.br>. Acesso em: 30 mar. 2024.

\_\_\_\_\_. Conselho Nacional de Justiça. *Resolução n. 363 de 12 de janeiro de 2021*. Estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais e a serem adotadas pelos tribunais. Disponível em: <https://www.cnj.jus.br>. Acesso em: 30 mar. 2024.

\_\_\_\_\_. Conselho Nacional de Justiça. *Tratamento de Dados Pessoais na Consulta de Jurisprudência: Desafios e Perspectivas*. 2021. Disponível em: <https://www.cnj.jus.br/wp-content/uploads/2022/02/tratamento-dados-pessoais-consulta-jurisprudencia30-11-21.pdf>. Acesso em: 5 jul. 2024.

\_\_\_\_\_. Conselho Superior de Justiça do Trabalho. *Resolução n. 241 de 31 de maio de 2019*. Altera a Resolução CSJT n. 185, de 24 de março de 2017, que dispõe sobre a padronização do uso, governança, infraestrutura e festão do Sistema Processo Judicial Eletrônico (PJe) instalado na Justiça do Trabalho. Disponível em: <<https://juslaboris.tst.jus.br/handle/20.500.12178/156430>>. Acesso em: 30 mar. 2024.

\_\_\_\_\_. Conselho Superior de Justiça do Trabalho. *Resolução n. 139 de 24 de junho de 2014*. Dispõe sobre medidas a serem adotadas pelos Tribunais Regionais do Trabalho para impedir ou dificultar a busca de nome de empregados com o fim de elaboração de “listas sujas”. Disponível em: <<https://juslaboris.tst.jus.br/handle/20.500.12178/39800>>. Acesso em: 30 mar. 2024.

\_\_\_\_\_. Conselho Superior de Justiça do Trabalho. *Resolução n. 185 de 24 de março de 2017*. Dispõe sobre a padronização do uso, governança, infraestrutura e festão do Sistema Processo Judicial Eletrônico (PJe) instalado na Justiça do Trabalho e dá outras providências. Disponível em: <https://juslaboris.tst.jus.br/handle/20.500.12178/102716>. Acesso em: 30 mar. 2024.

\_\_\_\_\_. Conselho da Justiça Federal. *Enunciado 681*. Disponível em: <<https://www.cjf.jus.br>>. Acesso em: 30 mar. 2024.

\_\_\_\_\_. Conselho da Justiça Federal. *Enunciado 688*. Disponível em: <<https://www.cjf.jus.br>>. Acesso em: 30 mar. 2024.

\_\_\_\_\_. *Decreto-lei n. 3.689, de 3 de outubro de 1941*. Código de Processo Penal. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/decreto-lei/del3689.htm](https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm)>. Acesso em: 25 maio 2021.

\_\_\_\_\_. *Lei n. 12.965/2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/112965.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm)>. Acesso em: 2 jan. 2021.

\_\_\_\_\_. *Lei n. 13.709/2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/113709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm)>. Acesso em: 2 jan. 2021.

\_\_\_\_\_. *Lei n. 13.793/2019*. Altera as Leis n.ºs 8.906, de 4 de julho de 1994, 11.419, de 19 de dezembro de 2006, e 13.105, de 16 de março de 2015 (Código de Processo Civil), para assegurar a advogados o exame e a obtenção de cópias de atos e documentos de processos e de procedimentos eletrônicos. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2019/lei/113793.htm](https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/113793.htm)>. Acesso em: 1 nov. 2021.

\_\_\_\_\_. *Lei n. 13.105, de 16 de março de 2015*. Código de Processo Civil. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2015/lei/113105.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/113105.htm)>. Acesso em: 25 maio 2021.

\_\_\_\_\_. *Lei n. 10.406, de 10 de janeiro de 2002*. Código Civil. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/leis/2002/110406compilada.htm](https://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm)>. Acesso em: 25 maio 2021.

\_\_\_\_\_. *Lei n. 14.289/2022*. Torna obrigatória a preservação do sigilo sobre a condição de pessoa que vive com infecção pelos vírus da imunodeficiência humana (HIV) e das hepatites crônicas (HBV e HCV) e de pessoa com hanseníase e com tuberculose, nos casos que estabelece; e altera a Lei n.º 6.259, de 30 de outubro de 1975. Disponível em:

<[https://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2022/lei/114289.htm](https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/114289.htm)>. Acesso em: 4 jan. 2022.

\_\_\_\_\_. Superior Tribunal de Justiça. *Agravo em Recurso Especial 1301454 ES 2018/0128396-4*. Relator: Ministro Lázaro Guimarães (Desembargador convocado do TRF 5ª Região), Diário de Justiça Eletrônico, Brasília, 27 jun. 2018. Disponível em: <http://stj.jus.br>. Acesso em: 23 maio 2021.

\_\_\_\_\_. Superior Tribunal de Justiça. *Rcl: 5072 AC 2010/0218306-6*. Relator: Ministro Marco Buzzi, Data de Julgamento: 11/12/2013, S2 - Segunda Seção, Data de Publicação: DJe 04/06/2014. Disponível em: <http://www.stj.jus.br>. Acesso em: 25 mar. 2024.

\_\_\_\_\_. Superior Tribunal de Justiça. *Recurso Especial de n. 1.316.921/RJ*. Relatora Ministra Nancy Andrighi. Recorrente: Google Brasil Internet. Recorrida: Maria da Graça Xuxa Meneghel. Disponível em: <http://www.stf.jus.br>. Acesso em 25 mar. 2024.

\_\_\_\_\_. Superior Tribunal de Justiça. *AREsp: 2130619 SP 2022/0152262-2*. Data de Julgamento: 07/03/2023, T2 - Segunda Turma. Data de Publicação: DJe 10/03/2023. Disponível em: [www.stj.jus.br](http://www.stj.jus.br). Acesso em: 29 abr. 2024.

\_\_\_\_\_. Superior Tribunal de Justiça. *AREsp: 1301454 ES 2018/0128396-4*. Relator: Ministro Lázaro Guimarães (Desembargador convocado do TRF 5ª Região). Data de Publicação DJ 27 de jun. 2018. Disponível em: <http://www.stj.jus.br>. Acesso em: 25 mar. 2024.

\_\_\_\_\_. Superior Tribunal de Justiça. *REsp 1660168/RJ*. Rel. Ministra Nancy Andrighi. Rel. para Acórdão Ministro Marco Aurélio Bellizze, Terceira Turma, julgado em 08/05/2018, DJe 05/06/2018. Disponível em: <http://www.stj.jus.br>. Acesso em: 25 mar. 2024.

\_\_\_\_\_. Supremo Tribunal Federal. Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.390. Relator: Ministro Rosa Weber. Plenário. Julgado em 7 de maio de 2020. Disponível em: <http://stf.jus.br>. Acesso em: 25 out. 2021.

\_\_\_\_\_. Supremo Tribunal Federal. Segunda Turma. *Agravo Regimental no HC 119.538/SP*. Relator: Min. Celso de Melo. Julgado em 22 de outubro de 2013. Disponível em: <http://www.stf.jus.br>. Acesso em: 25 mar. 2024.

\_\_\_\_\_. Supremo Tribunal Federal. *Agravo em Recurso Extraordinário de n. 1307386*. Relatora Ministra Carmem Lucia. Disponível em: <http://stf.jus.br>. Acesso em: 15 abr. 2024.

BULZICO, Bianca Amorim; SOUSA, Devilson da Rocha. *O princípio da publicidade dos atos processuais e as novas regras de privacidade e proteção de dados pessoais no Brasil*. Revista Brasileira de Políticas Públicas, v. 12, n. 3, p. 145-161, 2022.

CANOTILHO, José Joaquim Gomes. Dogmática de direitos fundamentais e direito privado. In: SARLET, Ingo Wolfgang (Org). *Constituição, Direitos Fundamentais e Direito Privado*. 2. ed. Porto Alegre: Livraria do Advogado, 2006.

CARDOSO, Oscar Valente. Lei Geral de Proteção de Dados e Publicidade Processual. *Jusbrasil*, 2020. Disponível em: <https://ovcardoso.jusbrasil.com.br/artigos/883957607/lei-geral-de-protecao-de-dados-e-publicidade-processual>. Acesso em: 3 jan. 2021.

COELHO, Luciano Augusto de Toledo. Testes psicológicos e o Direito: uma aproximação à luz da dignidade da pessoa humana e dos direitos da personalidade. *Psicol. Soc.*, Porto Alegre, v. 16, n. 2, p. 90-100, ago. 2004. Disponível em: [http://www.scielo.br/scielo.php?script=sci\\_arttext&pid=S0102-71822004000200011&lng=en&nrm=iso](http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0102-71822004000200011&lng=en&nrm=iso). Acesso em: 10 jan. 2021.

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 (Org.). *Lei Geral de Proteção de Dados (Lei n. 13.709/2018)*. A caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020, p. 199-210.

DIAS, José Aléssio de Freitas. *Compliance Officer no Brasil: uma visão sobre a responsabilidade criminal do Chief Compliance, ante a existência de um programa de integridade e a assunção da função garante*. Dissertação (Mestrado) - Programa de Pós-Graduação do Instituto de Direito Público, Escola de Administração de Brasília. Brasília, 2019.

DIDIER JUNIOR, Fredie. *Curso de Direito Processual Civil*. 24. ed. Salvador: Juspodium, 2022, v. 1.

DINIZ, Maria Helena. *Dicionário jurídico*. São Paulo: Saraiva, 1998.

DIRSCHERL, Fernanda Pantaleao; FALEIROS JÚNIOR, José Luiz. Dados pessoais sensíveis sobre gênero. Breve análise. *Migalhas*, 15 mar. 2024. Disponível em <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/403508/dados-pessoais-sensiveis-sobre-genero-breve-analise>. Acesso em: 29 abr. 2024.

DISTRITO FEDERAL. TJ-DFT. 3ª Turma. *Processo n. 0707858-40.2021.8.07.0000*. Agravante: Josyellen Crysthyna Martins de Araujo. Agravados: Bruno Alvarenga Silva Loredó, Instituto da Face e Otorrinolaringologia Ltda e Rede D'OR São Luiz S.A. Relatora: Des. Fátima Rafael. Julgado em 09/06/2021. Publicado no DJE 23.06.2021. Disponível em: <https://pesquisajuris.tjdft.jus.br/IndexadorAcordaos-web/sistj>. Acesso em: 29 mar. 2024.

\_\_\_\_\_. TJ-DFT. 7ª Turma Cível. *Processo n. 0710842-94.2021.8.07.0000*. Agravante: Jose Celso Valadares Gontijo e Ana Maria Baeta Valadares Gontijo. Agravados: BRB Banco de Brasília S.A. Relator: Des. Fabio Eduardo Marques. Julgado em 25/08/2021. Publicado no DJE 18.08.2021. Disponível em <https://pesquisajuris.tjdft.jus.br/IndexadorAcordaos-web/sistj>. Acesso em: 29 mar. 2024.

DONEDA, Danilo *et al.* (Coord.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021.

DONEDA, Danilo. MACHADO, Diogo. Interconexão de bancos de dados governamentais e a garantia da privacidade e proteção de dados pessoais sob a perspectiva do Decreto

10.046/2019. In: SCHERTEL, Laura; ALVES JR, Sérgio; DONEDA, Danilo (Org.). *Internet e regulação*. São Paulo: Saraiva: 2021, p.326-352

FACCHINI NETO, E.; DEMOLINER, K. S. Direito à Privacidade e Novas Tecnologias: breves considerações acerca da proteção de dados pessoais no Brasil e na Europa. *Revista Internacional Consinter De Direito*, v. 4, n. 7, p. 19-40, 2018.

FALEIROS JÚNIOR, José Luiz de Moura. *Precedente C-59/22 do Tribunal de Justiça da União Europeia (TJUE): Necessidade de Prova para indenização por violação de dados pessoais*. Migalhas, 15 mar. 2024. Disponível em <<https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/410393/precedente-c-590-22-tjue-indenizacao-por-violacao-de-dados-pessoais>>. Acesso em: 12 jul. 2024.

FARIA, Edimur Ferreira de Faria; SOUZA, Livia Maria Cruz Gonçalves de. Governança Corporativa na Administração Pública Brasileira: Um processo em construção! *Revista Jurídica Direito & Paz*, Lorena-SP, ano IX, n. 37, p. 273-292, 2017. Disponível em: [https://www.mpsp.mp.br/portal/page/portal/documentacao\\_e\\_divulgacao/doc\\_biblioteca/bibli\\_servicos\\_produtos/bibli\\_informativo/bibli\\_inf\\_2006/6FC8373CC2389118E050A8C0DD016FCF](https://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_informativo/bibli_inf_2006/6FC8373CC2389118E050A8C0DD016FCF). Acesso em: 20 jan. 2024.

FERRAZ JÚNIOR, Tercio Sampaio. *Introdução ao Estudo do Direito: técnica, decisão, dominação*. 3. ed. São Paulo: Atlas, 2001.

\_\_\_\_\_. Comunicação de Dados e Proteção ao Sigilo. In: CUEVA, Ricardo Villas Bôas; DONEDA, Danilo; MENDES, Laura Schertel (Org.). *Lei Geral de Proteção de Dados (Lei n. 13.709/2018)*. A caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020, p. 165-176.

GOMES JUNIOR, Luiz Manoel; FERREIRA, Jussara Suzi Assis Borges Nasser. O Segredo de Justiça no Novo Código de Processo Civil: análise das principais inovações. *Revista de Processo*, v 250, p. 133-146, 2015.

HIRATA, Alessandro. Direito à privacidade. In: CAMPILONGO, Celso Fernandes; GONZAGA, Alvaro de Azevedo; FREIRE, André Luiz (Coord.). *Enciclopédia jurídica da PUC-SP*. Tomo: Direito Administrativo e Constitucional. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: <https://enciclopediajuridica.pucsp.br/verbete/71/edicao-1/direito-a-privacidade>. Acesso em 17 jan. 2021.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. *Fundamentos de Metodologia da Pesquisa*. 7. ed. São Paulo: Atlas, 2010.

LONGHI, João Victor Rozatti ; FALEIROS JÚNIOR, José Luiz de Moura; MARTINS, Guilherme Magalhães. A pandemia da covid-19, o “profiling” e a Lei Geral de Proteção de Dados. *Migalhas*, 28 abr. 2020. Disponível em: <https://www.migalhas.com.br/depeso/325618/a-pandemia-da-covid-19--o--profiling--e-a-lei-geral-de-protecao-de-dados>. Acesso em: 20 jan. 2023.

LONGHI, João Victor Rozatti ; MARTINS, Guilherme Magalhães. Dados pessoais, covid-19 e MP 954/20 2020. *Migalhas*, 07 maio 2020. Disponível em: <https://www.migalhas.com.br/depeso/326242/dados-pessoais--covid-19-e-a-mp-954-20>. Acesso em: 20 jan. 023.

MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz; MITIDIERO. *Novo Código de Processo Civil Comentado*. 2. ed. São Paulo: Editora Revista dos Tribunais, 2016.

MARTINS, Fladimir Jerônimo Belinati. *Dignidade da pessoa humana: princípio constitucional fundamental*. Curitiba: Juruá, 2009.

MASSENO, Manuel David. *A Segurança no Tratamento de Dados Pessoais no Sistema Judicial, em Portugal e no Brasil*. Revista do Cejur: Prestação jurisdicional, Florianópolis, v. 9, e367, p. 01-09, 2021. Disponível em: <https://revistadocejur.tjsc.jus.br>; Acesso em 5. Jul. 2024.

MENDES, Laura Schertel; RODRIGUES Jr., Otavio Luiz; FONSECA, Gabriel Campos Soares da. O Supremo Tribunal Federal e a proteção Constitucional dos dados pessoais: Rumo a um direito fundamental autonomo. *In: MENDES, Laura Schertel et al* (Coord). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021, p. 61-71.

MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares da. Proteção de dados para além do consentimento: Tendências de materialização. *In: MENDES, Laura Schertel et al* (Coord). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021, p. 73-95.

MORAES, Maria Celina Bodin de. *Danos à pessoa humana: uma leitura civil-constitucional dos danos morais*. Rio de Janeiro: Renovar, 2003.

NEGRÃO, Antonio Carlos. Economia Digital, Proteção de Dados e Competitividade. *In: CUEVA, Ricardo Villas Bôas; DONEDA, Danilo; MENDES, Laura Schertel* (Org.). *Lei Geral de Proteção de Dados (Lei n. 13.709/2018)*. A caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020, p. 29-38.

NÓBREGA MALDONADO, Viviane (Coord). *LGPD: Lei Geral de Proteção de Dados Pessoais - manual de implementação*. São Paulo: Thomson Reuters Brasil, 2019.

OLIVEIRA, Paulo Eduardo Vieira. SILVA, Fabrício Lima. *O aparente paradoxo entre a política de open justice e o direito fundamental à proteção de dados*. Revista Eletrônica do TRT-PR. Curitiba.: TRT 9ª Região, V,12, n. 118. Mar. 2023. Disponível em: [https://juslaboris.tst.jus.br/bitstream/handle/20.500.12178/215739/2023\\_oliveira\\_paulo\\_aparente\\_paradoxo.pdf?sequence=2&isAllowed=y](https://juslaboris.tst.jus.br/bitstream/handle/20.500.12178/215739/2023_oliveira_paulo_aparente_paradoxo.pdf?sequence=2&isAllowed=y); Acesso em 5. Jul. 2024.

ONU. *Declaração Universal dos Direitos Humanos*. Adotada e proclamada pela Assembleia Geral das Nações Unidas (resolução 217 A III) em 10 de dezembro de 1948. Disponível em: <https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>. Acesso em: 26 jun. 2021.

PORTUGAL. Ministério Público. *DL n. 47344/66, de 25 de novembro*. Código Civil. Disponível em:



[https://www.pgdlisboa.pt/leis/lei\\_mostra\\_articulado.php?nid=775&tabela=leis](https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=775&tabela=leis). Acesso em: 20 jan. 2023.

PORTUGAL. *Critérios de seleção, anonimização e publicação de jurisprudência ECLI. Parecer sobre os critérios de seleção, tratamento, apresentação e arquivo de decisões judiciais na base de dados de tratamento de informação legal (ECLI)*. Conselho Superior da Magistratura. 2020. Disponível em: <https://www.redecivil.csm.org.pt/wp-content/uploads/2020/01/PROTEC%C3%87%C3%83O-DE-DADOS-E-PROCESSO-CIVIL-Isabel-C-teixeira.pdf> Acesso em: 7 jul. 2024.

\_\_\_\_\_. Supremo Tribunal de Justiça. *Acórdão n.º 403/2015*. Processo n. 773/15. Plenário. Relator Conselheiro Lino Rodrigues Ribeiro. Julgamento em 27 de agosto de 2015. Disponível em: [www.stj.pt](http://www.stj.pt). Acesso em: 28 abr. 2024.

\_\_\_\_\_. Supremo Tribunal de Justiça. *Acórdão n.º 720/2022*. Processo n. 836/21. Plenário. Relator: Conselheiro Lino Rodrigues Ribeiro. Julgamento em 3 de novembro de 2022. Disponível em: [www.stj.pt](http://www.stj.pt). Acesso em: 29 abr. 2024.

PULIDO, Carlos Bernal. A fundamentalidade dos direitos fundamentais. In: ASENSI, Felipe Dutra; DE PAULA, Daniel Giott (Coordes.). *Tratado de Direito Constitucional: constituição, política e sociedade*. Rio de Janeiro: Elsevier, 2014.

ROCA, Alejandro Rodeiguez. *La Protección de Datos Personales em la Administración de Justicia*. Tese de doutoramento. Universidad Internacional de La Rioja. 2020.

ROCHA, Henrique de Moraes Fleury da. Garantias Fundamentais do processo sob a ótica da informatização judicial. *Revista de Processo*, v. 267, p. 129-170, 2017.

ROSEVALD, Nelson. A LGPD e a despersonalização da personalidade. Disponível em <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/350374/a-lgpd-e-a-despersonalizacao-da-personalidade> . Acesso em 1 nov. 2021.

SANTOS, Luciano Alves dos. *A Lei Geral de Proteção de Dados Pessoais e os seus reflexos no Poder Judiciário brasileiro*. “Privacy and Data Protection Magazine”, Lisboa. Privacy and Data Protection Magazine. ISSN 2184 -920X, n.º 1 (2021), pp. 92 -107.

SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais*. 6. ed. Porto Alegre: Livraria do Advogado, 2006.

\_\_\_\_\_. Notas acerca do assim chamado direito ao esquecimento na jurisprudência do Superior Tribunal de Justiça Brasileiro In: CUEVA, Ricardo Villas Bôas; DONEDA, Danilo; MENDES, Laura Schertel (Org.). *Lei Geral de Proteção de Dados (Lei n. 13.709/2018)*. A caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020, p. 65-90.

SILVA, José Afonso da. *Comentário Contextual à Constituição*. 2. ed. São Paulo: Malheiros, 2006.

SOUSA SANTOS, Boaventura de. Os tribunais e as novas tecnologias de comunicação e de informação. *Sociologias*, Porto Alegre, n. 13, p. 82-109, jun. 2005. Disponível em: <[http://www.scielo.br/scielo.php?script=sci\\_arttext&pid=S1517-45222005000100004&lng=en&nrm=iso](http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1517-45222005000100004&lng=en&nrm=iso)>. Acesso em: 10 jan. 2023.

TEFFÉ, Chiara Spadaccini de. *Dados pessoais sensíveis: qualificação, tratamento e boas práticas*. Indaiatuba-SP: Foco, 2022.

TEIXEIRA, Isabel Maria Curto. Proteção de Dados e Processo Civil. *Recentes Alterações Legislativas e Novas Problemáticas*. Disponível em: <https://www.redecivil.csm.org.pt/wp-content/uploads/2020/01/PROTEC%C3%87%C3%83O-DE-DADOS-E-PROCESSO-CIVIL-Isabel-C-teixeira.pdf>. Nov. 2019. Acesso em: 11 jul. 2024.

WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo poder público. In: MENDES, Laura Schertel *et al.* (Coord). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021, p. 271-288.

ZANETTI, Dânton. Proteção de dados pessoais e publicidade processual: Um contrassenso? *Portal Migalhas*, 15 abr. 2021. Disponível em: <<https://www.migalhas.com.br/depeso/343796/protecao-de-dados-pessoais-e-publicidade-processual-um-contrassenso>>. Acesso em: 4 jan. 2022.