

“Ainda existem juízes em Berlim”: a interpretação judicial e o surgimento de um direito fundamental à proteção de dados pessoais

“There are still judges in Berlin”: judicial interpretation and the emergence of a fundamental right to personal data protection

Marlon Gabriel Dos Santos¹ 

¹Acadêmico do Curso de Direito – Universidade Estadual do Oeste do Paraná (UNIOESTE), Campus de Marechal Cândido Rondon

RESUMO

A revolução tecnológica das últimas décadas impactou não apenas a economia mundial, mas também a comunicação, dando às máquinas e ao processamento de dados pessoais uma centralidade ostensiva. Em decorrência disso, surgiu um debate global sobre a privacidade, a intimidade e a proteção de dados pessoais, nesse novo contexto. Restrito ao caso brasileiro, este trabalho, partindo de marcos normativos como a Constituição, a Lei 12.965/2014, a Lei 13.709/2018, os precedentes dos Tribunais e os paradigmas doutrinários, buscou reconstituir a via percorrida pela interpretação judicial criativa que reconheceu um direito fundamental à proteção de dados pessoais, antes mesmo da sua previsão expressa com o advento da emenda constitucional nº 115/2022. Isso posto, utilizou-se uma metodologia analítica-dedutiva, concluindo-se que a hermenêutica criativa do Judiciário, na temática, mostrou-se adequada para a concretização do direito fundamental em análise, sem depender da positividade expressa como pressuposto da sua aplicação.

Palavras-chave: Direitos fundamentais; Hermenêutica; LGPD; Marco Civil da Internet; Proteção de dados.

ABSTRACT

The technological revolution of recent decades has impacted not only the global economy but also communication, giving machines and personal data processing a prominent role. As a result, a global debate has emerged regarding privacy, intimacy, and the protection of personal data in this new context. Focusing on the Brazilian case, this study, based on legal frameworks such as the Constitution, Law 12.965/2014, Law 13.709/2018, court precedents, and doctrinal paradigms, sought to reconstruct the path taken by creative judicial interpretation that recognized a fundamental right to personal data protection even before its explicit provision with the advent of Constitutional Amendment No. 115/2022. In doing so, an analytical-deductive methodology was employed, leading to the conclusion that the judiciary's creative hermeneutics in this area proved suitable for realizing the fundamental right under analysis, without relying on express legislative enactment as a prerequisite for its application.

Keywords: Fundamental Rights; Hermeneutics; LGPD; Internet Civil Framework; Data Protection.

1 Introdução

A revolução tecnológica das últimas décadas alterou, exponencialmente, a forma humana de comunicação, e deu às máquinas uma centralidade a todo esse processo. Os efeitos dessa revolução não ficaram restritos às comunicações, mas estenderam-se para a economia mundial, inclusive, para um profícuo debate global sobre a privacidade, a intimidade e a proteção de dados pessoais.

O presente estudo versa sobre alguns aspectos gerais dessa nova realidade mundial e, mais especificamente, sobre os debates jurídicos decorrentes do processamento em massa de dados pessoais e de como a interpretação judicial criativa foi crucial para construir um direito fundamental à proteção de dados e da personalidade, frente aos efeitos adversos de abusos que instrumentalizaram a tecnologia. Partindo de referências normativas, doutrinárias e jurisprudenciais buscou-se reconstituir e compreender a via percorrida pelo Poder Judiciário, especialmente nos Tribunais, no reconhecimento e construção do direito fundamental à proteção de dados pessoais, antes mesmo da sua previsão expressa no inciso LXXIX, do Art.5º da Constituição Federal (CF).

Ainda quando não havia uma previsão constitucional expressa sobre o direito fundamental à proteção de dados pessoais, outros preceitos como a privacidade, a intimidade e às disposições da Lei Geral de proteção de dados pessoais (LGPD) e do Marco Civil da internet, serviram como garantidores jurídicos oponíveis a terceiros, inclusive ao Estado, conforme reconheceram os Tribunais. De tal sorte, o Cidadão, tão logo verificasse uma ação ou omissão (lesivas aos seus direitos de personalidade) encontrava uma Magistratura receptiva à boa eficácia dos direitos particulares envolvidos, de modo semelhante ao que fez o *Moleiro de Sans-Souci*, na obra de François Andrieux, ao proclamar a expressão “ainda existem juizes em Berlim”. Inferindo-se que o papel dos Juizes na sociedade democrática está ligado à noção de garantia aos direitos assegurados pela ordem jurídica, demandando uma expectativa do Cidadão, na atuação judicial, como meio de coibir abusos e excessos, inclusive do próprio Estado.

De outra parte, cabe destacar que nenhum dos direitos que serão aqui discutidos são absolutos, estando os seus conflitos com outros direitos da vida em sociedade, em última instância, suscetíveis a um posicionamento judicial.

Com efeito, o trabalho buscou compreender como os Tribunais brasileiros construíram as primeiras bases para uma efetiva eficácia de um direito fundamental à proteção aos dados pessoais no Brasil, naquilo que antecedeu a previsão do inciso LXXIX, do Art.5º da CF, com o advento da emenda constitucional nº 115/2022. Para tanto, utilizou-se uma metodologia analítico-descritiva sobre as referências discriminadas ao final da pesquisa.

2 A Revolução das Comunicações e o Delinear de um Novo Direito Fundamental

2.1 Generalidades

Não se pode ignorar a evolução exponencial dos computadores, nas últimas décadas, e os expressivos impactos das novas tecnologias, erigidas sobre a infraestrutura da internet. O mundo contemporâneo, por evidente, já é produto dessas transformações tecnológicas, a exemplo, haja vista a assertiva da revista *The economist*: “o recurso mais valioso do mundo não é mais o petróleo, mas os dados” (THE ECONOMIST, 2017). De tal sorte, o sistema capitalista já se estruturou sobre as novas variantes tecnológicas e, nesse sentido, Unger (2018) já descreve a atual prática mais avançada de produção como sendo a economia do conhecimento, ao revés da declinante indústria de produção em massa. Para o autor,

a economia do conhecimento consiste na acumulação de capital, tecnologia, capacitações tecnológicas e ciência aplicados à condução das atividades produtivas. Sua característica ideal é a inovação permanente em processos e métodos, assim como em produtos e tecnologias [...] se propõe ser um paradigma de produção que continuamente reinventa a si mesma (UNGER, 2018, p. 26).

Além disso, Castells (1999) ensina que, diante do novo modo informacional de desenvolvimento, “a fonte de produtividade acha-se na tecnologia de geração de conhecimentos, de processamento de informações e de comunicação de símbolos” (CASTELLS, 1999, p. 53). Destarte, assim como Unger (2018) entende a economia do conhecimento como algo que se reinventa continuamente, Castells (1999) entende que as novas tecnologias são processos em desenvolvimento, nos quais a figura do usuário as redefine, e acabam por se confundir com a figura do criador. Ademais, a capacidade dos sistemas de comunicação, dos computadores, da decodificação, entre outros, dadas as suas capacidades de criação e de manipulação de símbolos, além da capacidade de produzir e distribuir bens e serviços, constituem-se em verdadeiros amplificadores e extensões de tarefas, antes apenas restritas à mente humana (CASTELLS, 1999).

Ciências Sociais Aplicadas em Revista, v. 28, n. 48, p. 356-380, Edição Especial, 2024.

Atualmente, ao se abordar o tema do processamento de dados, vai longe o tempo de pessoas entediadas analisando arquivos de papel. Ao contrário, o colossal alcance do processamento de informações é bem explicado pela definição de big data que é entendido como: “conjunto de técnicas que permitem analisar, processar e gerenciar conjuntos de dados extremamente grandes que podem ser analisados informaticamente para revelar padrões, tendências e associações, especialmente em relação à conduta humana e às interações dos usuários” (REAL ACADEMIA, 2020, tradução nossa). Como destaca Pessoa (2020), com a obtenção desses dados em larga escala é possível que governos e corporações passem a vigiar e a identificar padrões em indivíduos ou massas populacionais, sem deixar de considerar outros pontos como a velocidade do processamento, a variedade, a veracidade (confiabilidade) e valor (benefício decorrente) do processamento dos dados coletados.

Conforme já salientado, o processamento de dados não serve apenas ao setor privado, mas, igualmente, ao poder público. Este último se utiliza daquele instrumento para a persecução de políticas públicas, serviços e, inclusive, a promoção da segurança nacional. Sobretudo, o Direito já se debruça, por muito tempo, sobre os impactos da evolução tecnológica nos direitos e na personalidade dos indivíduos e, sobretudo, em como proteger o indivíduo de abusos e de excessos, tanto pelo Estado quanto por particulares. Quiçá, o mais lembrado marco histórico dessa preocupação seja o texto estadunidense “*The right to the privacy*”, publicado em 1890, escrito por Warren e Brandeis, versando sobre o desenvolvimento do mercado de informações e notícias e seus aspectos invasivos à intimidade das pessoas. Com efeito, defenderam um “direito de estar sozinho” e, vinculando à privacidade, por sua vez, como uma noção de liberdade combinada com a inviolabilidade da personalidade humana. O clássico artigo contribuiu para que aquele direito fosse constitucionalmente reconhecido em solo ianque (RUARO; MOLINARO, 2017).

Mais tarde, em 1983, o Tribunal Constitucional Federal alemão (*Bundesverfassungsgerichts*), na decisão em que costuma se referir como aquela que primeiro reconheceu um direito fundamental implícito à autodeterminação informativa, que é a prerrogativa individual de decidir sobre a divulgação e a utilização de seus dados pessoais. O Tribunal orientou-se pela leitura combinada do princípio da dignidade da pessoa humana e do direito ao livre desenvolvimento da personalidade, sendo o cerne da decisão a preocupação com a garantia da liberdade dos cidadãos em face da repressão estatal. Outra decisão, igualmente multicitada, foi

àquela de 1969 em que o Tribunal assentou que a Lei Fundamental proíbe a coleta compulsória com registro da inteira personalidade do ser humano (SARLET; SAAVEDRA, 2020).

A proteção de dados pessoais passou a receber proteção jurídico-normativa a partir da década de 1970, sobretudo no exterior, com as primeiras leis, tratados e decisões sobre o tema. A primeira geração dessas normas focou na autorização e no registro de bancos de dados diante dos órgãos respectivos, não sendo a privacidade da pessoa um aspecto principal, no entanto, foi apenas na quarta geração (década de 90 em diante) que essas normas passaram a perseguir uma proteção efetiva da privacidade individual, a exemplo a Diretiva de Proteção de Dados Pessoais 95/46/CE, de 1995, e o *General Data Protection Regulation* (GDPR), em vigor desde 2018, ambos da União Europeia (MARTINS; TATEOKI, 2019).

No Brasil, a proteção da privacidade, da intimidade, da vida privada e do sigilo das comunicações foram alçados à condição de direitos fundamentais (Art 5º, X e XII da CF), e, recentemente, passaram a integrar o ordenamento jurídico o Marco Civil da internet-MCI (Lei nº 12.965/2014) e a Lei Geral de proteção de dados Pessoais-LGPD (Lei nº 13.709/2018). Quanto a essa última, além de inspirada no GDPR europeu, é uma das decorrências de debates internos do Mercosul sobre o tema. Assim, a LGPD introduziu no Brasil um debate salutar de parâmetros globalmente aceitos na matéria (DONEDA, 2021), o que contribui para que o país seja inserido no rol de nações adequadas à proteção de dados e à privacidade, fomentando, inclusive, setores como a Tecnologia da Informação, haja vista que o Brasil poderá processar dados oriundos de países exigentes para com a proteção supracitada (MONTEIRO, 2018).

Ante o exposto, e, considerando-se o escopo a que se propõe este artigo, perfilha-se o entendimento de Schreiber (2021) de que a proteção de dados pessoais é um dos mais “sensíveis” desafios que o direito contemporâneo enfrenta, enquanto consequência dos avanços tecnológicos recentes. No próximo tópico será explorado como foi delineada a proteção de dados pessoais enquanto um direito autônomo e não, necessariamente, adstrito à privacidade, à intimidade ou o sigilo.

2.2 O Delinear do Direito Autônomo à Proteção de Dados Pessoais

O processamento de dados pessoais é acompanhado pelos riscos implícitos à pessoa titular dos dados (MENDES; DONEDA, 2018), daí também a compreensão do Tribunal Constitucional

Federal alemão de que no atual contexto de big data não há mais dados irrelevantes ou insignificantes, premissa já multicitada em votos no Supremo Tribunal Federal (STF). Reconhecendo-se, portanto, que o dado “público” ou “neutro” e, aparentemente isolado, passa a conter relevância quando combinado com outros dados, tornando-se apto à proteção jurídica na linha do que fora decidido na Ação Direta De Inconstitucionalidade (ADI) nº 6387/2020 (MENDES; RODRIGUES JR.; FONSECA, 2021).

A proteção de dados pessoais é oponível tanto aos particulares quanto ao Estado. O que se depreende é que o indivíduo seja o consumidor, seja o usuário de serviços ou, como cidadão, não renuncie a seus direitos, na lição de Schreiber (2021):

a proteção de seus dados pessoais, alcança qualquer ambiente onde tais dados circulem. Longe de representar “informações sem dono” livremente coletáveis na internet, os dados pessoais exprimem uma importante projeção da personalidade humana, exigindo firme proteção da ordem jurídica (SCHREIBER, 2021, p. 320).

No setor privado, quicá, um dos mais emblemáticos casos foi o escândalo da *Cambridge Analytica*, que usou dados pessoais de mais de 50 milhões de usuários do Facebook, sem o consentimento dessas pessoas, para fins de propaganda eleitoral, com elaboração de perfis individuais, por vezes, muito precisos, ou seja, para uma finalidade diversa da qual os dados foram obtidos, inicialmente, em um “teste psicológico” na rede social. O escândalo foi decorrência de uma displicência das políticas do Facebook sobre o uso e a fiscalização dos dados extraídos da plataforma, à época (BBC NEWS, 2018).

Em outra perspectiva, o processamento de dados pelo Poder Público também merece atenção para que os dados obtidos pelo Estado e as limitações possíveis para que isso não se transforme em um agigantamento e conseqüente abuso do poder estatal sobre os indivíduos. Note-se que as primeiras normas de proteção de dados pessoais (década de 1970) já possuíam como cerne a proteção de direitos, e liberdades fundamentais em face do Estado (WIMMER, 2021b). É notório o fato de que, cada vez mais, o Poder Público concentra e controla, mesmo que indiretamente, aspectos financeiros, dados da saúde, da Educação, das demandas judiciais e dados trabalhistas de todos os cidadãos, e a sua presença, cada vez mais digital, é pressuposto para a execução de diversas políticas públicas e para o cumprimento da missão do Estado, inclusive a segurança nacional (SOUSA; FRANCO, 2020). No entanto, o Estado não pode ser tido como uma “unidade

informativa” devendo os dados estarem submetidos, sempre que necessário, ao órgão específico e à finalidade que justificou sua coleta, pois não há, no ordenamento jurídico brasileiro, uma autorização irrestrita ao livre trânsito de dados pessoais entre repartições públicas (WIMMER, 2021a).

Dados os limites espaciais deste trabalho, não é possível elencar um número extenso de razões que contribuíram para que legisladores, doutrinadores e magistrados passassem a conjecturar ou elaborar entendimentos para a salvaguarda e para a regulação da proteção de dados pessoais e, inclusive, a depender do autor, afirmar a existência de um novo direito fundamental.

A propósito, é oportuno destacar que Carlos Maximiliano já afirmava que o legislador é mais um ator do que autor das transformações jurídicas, o legislador capta e é influenciado pelas mudanças e pelos cenários ao seu entorno “a natureza humana amolda as instituições jurídicas; por sua vez estas reagem sobre aquela” (MAXIMILIANO, 2003, p. 17). Na mesma linha, tem-se a lei, que pode advir de uma necessidade, previamente existente do jurisdicionado, isto é, “a lei não surge como fonte de direito pela vontade espontânea do legislador, mas sempre deve refletir um bem da vida ou uma regra de processo ou procedimento sobre os quais se sentiu necessidade de haver regulamentação” (PERILLI, 2020). Destarte, observa-se, nitidamente, esse padrão, no caso brasileiro, em que tanto o MCI quanto a LGPD supriram, mesmo que em parte, uma lacuna no ordenamento e, enquanto leis específicas, evitaram a “sobreconstitucionalização” das suas matérias (MENDES; RODRIGUES JR.; FONSECA, 2021). Ademais, nota-se que, sobretudo antes da LGPD, havia uma legislação carente e esparsa sobre o tema da proteção de dados pessoais (RUARO; MOLINARO, 2017).

Um dos debates mais interessantes no Direito Constitucional sobre a temática supracitada foi o delinear da existência de um direito fundamental implícito à proteção de dados pessoais na Constituição Federal de 1988 (CF). Esse direito conforme se depreendia de Sarlet e Saavedra (2020) seria autônomo e vinculado à proteção da personalidade, e não se confundiria com a privacidade ou com o sigilo da comunicação de dados, nem seria uma mera evolução da primeira.

Para reconhecer a proteção de dados pessoais como direito fundamental Sarlet e Saavedra (2020) partiram de uma reflexão filosófica segundo a qual o Direito é estruturado, a partir do fundamento da “vontade livre”. A saber, “somente serão institucionalizados aqueles avanços, aquelas ampliações das esferas de reconhecimento recíproco, que forem expressões da liberdade” (SARLET; SAAVEDRA, 2020, p. 38). Assim, os autores, sustentaram que a proteção de dados

pessoais e o seu reconhecimento como direito fundamental daria um novo e atual sentido à proteção da pessoa, à dignidade e, sobretudo, às liberdades que lhes são próprias.

No campo do direito positivo, Mendes (2020) destacou que a tutela de direito fundamental implícito à proteção de dados pessoais podia ser extraída de uma interpretação conjunta das normas constitucionais, como o princípio da dignidade da pessoa humana (Art. 1º, III), inviolabilidade da vida privada (Art. 5º, X) e a garantia processual do habeas data (Art. 5º, LXXII). Sobre esse último é relevante a interpretação adotada pelo ministro Gilmar Mendes de que “nós temos o habeas data com o propósito, o intento de tutelar aquilo que entendemos ser uma proteção da autonomia privada nesse âmbito da autodeterminação sobre os dados” (BRASIL, 2015, p. 35). Naquela oportunidade, o STF, no Recurso Extraordinário (RE) nº 673.707/2015 (*leading case*), afastou a visão reducionista da garantia do habeas data, reconhecendo o seu amplo espectro na Constituição pós-positivista de 1988. Nesse julgado, o Tribunal assentou que o habeas data permite a obtenção de dados referentes ao pagamento de tributos do próprio contribuinte, em quaisquer sistemas informatizados dos órgãos fazendários (BRASIL, 2015). O posicionamento se aproximou muito do reconhecimento da autodeterminação informativa, circunstância em que considerada a atual realidade do processamento em massa de dados pessoais: “o indivíduo se mostra capacitado e informado o suficiente para exercer sua liberdade de decisão acerca do tratamento efetuado junto aos seus dados” (NOGUEIRA; FONSECA, 2020, p. 22). Observa-se que, posteriormente, a autodeterminação informativa foi positivada pela LGPD como fundamento da disciplina da proteção de dados pessoais (Art. 2º, II), seguindo o que já defendiam os estudiosos do tema.

Definidas essas premissas, no próximo tópico deste trabalho pretende-se expor e compreender a importância e a atuação do Poder Judiciário, notadamente dos Tribunais, na tutela e na aplicação das matérias do MCI e da LGPD, sem dissociação dos recortes constitucionais e das questões até o momento abordadas.

3 O Poder Judiciário Enquanto Garantidor de Direitos

3.1 Da Importância e da Atuação do Judiciário na Construção de uma Proteção à Dados Pessoais

No séc. XVIII o escritor François Andrieux, escreveu o texto intitulado *Le meunier Sans-Souci* ou “*O moleiro de Sans-Souci*”. A narrativa descreve, em síntese, o interesse do déspota esclarecido Frederico II, O Grande, rei da Prússia, em expandir os domínios do seu palácio em uma

Ciências Sociais Aplicadas em Revista, v. 28, n. 48, p. 356-380, Edição Especial, 2024.

tranquila região, no entanto, um moinho estava atrapalhando tal propósito e o seu dono, um simples moleiro, resistia à ideia de vendê-lo ao rei por razões sentimentais. Não contente com a situação, Frederico II mandou que trouxessem o moleiro a sua presença e, ao perceber a resistência do súdito, chegou a dizer que poderia retirar-lhe o moinho sem nenhuma contrapartida indenizatória. O moleiro, ao ouvir isso, retrucou dizendo que nem mesmo o rei pode fazer tal coisa pois “ainda existem juízes em Berlim”. E o rei se mostrou tão contente por saber que o povo acreditava na justiça que logo desistiu de intervir no moinho (ANDRIEUX, 2021). Modernamente, a história pode ser interpretada como símbolo da prevalência do império da lei sobre o arbítrio dos governantes e a confiança da sociedade no Poder Judiciário, vez que “se necessário, terá suas causas processadas e julgadas de maneira sensata, com segurança, destemor, presteza e justiça, independentemente de quem esteja no outro lado da relação jurídica processual” (VIANNA, 2018, p. 65). Ao lado disso Steiner (2020), ao versar sobre o papel dos juízes na sociedade democrática, afirma que eles são os garantidores dos direitos que são assegurados a todos e a cada um.

Com base nesses pressupostos da jurisdição e, considerando-se que leis específicas sobre a proteção de dados pessoais são recentíssimas, pode-se inferir que, no Brasil, também se reproduziu um padrão, perceptível em outros países, de que um direito à proteção de dados pessoais foi se apresentando como resposta a demandas concretas, que foram atendidas com os instrumentos gerais disponíveis no respectivo ordenamento e sem depender, portanto, dessa ou daquela área específicas do direito (DONEDA, 2021). Prova disso é que algumas das demandas judiciais a serem expostas a seguir não aguardaram as recentes leis temáticas da internet e da proteção de dados. Mesmo assim, o Judiciário foi chamado a julgá-las utilizando os instrumentos normativos disponíveis até então. A assertiva a respeito da importância de um Judiciário atuante a favor do direito em comento, pode ser assim sintetizada, conforme Ruaro e Molinaro (2017):

em face do panorama brasileiro, cabe, então, ao Poder Judiciário tutelar a pretensão daqueles que pretendam ver seus dados pessoais protegidos, quer seja na relação de particulares, quer seja na seara do direito público tarefa esta que enseja uma interpretação sistemática a partir da Constituição Federal, dos diplomas legais existentes e dos princípios informadores (RUARO; MOLINARO, 2017, p. 31).

Quiçá, um dos aspectos mais interessantes na evolução da trajetória brasileira na proteção de dados pessoais, sob a vigência da CF de 1988, seja a evolução do entendimento do STF sobre as disposições constitucionais pertinentes. Note-se que, inicialmente, a Suprema Corte aplicava a

tese defendida¹ pelo professor Tércio Sampaio Ferraz Jr., segundo a qual “[o] sigilo não é o bem protegido, não é o objeto do direito fundamental [...] o objeto protegido no direito à inviolabilidade do sigilo não são os dados em si, mas a sua comunicação restringida (liberdade de negação)” (FERRAZ JR., 1993, p. 443-7, grifo nosso). E assim, foi se delineando a posição presente em alguns julgados como no Mandado de Segurança (MS) n° 21.729/2001 e mais notadamente no RE n° 418.416/2006 e no habeas corpus (HC) n° 91.867/2012. Sobre esse penúltimo, o STF, na relatoria do ministro Sepúlveda Pertence, entendeu que um mandado de busca e apreensão, ao alcançar um microcomputador, não hostilizou a garantia da inviolabilidade do domicílio da empresa, pois a proteção constitucional do Art. 5º, XII não recai sobre os dados em si, mas sobre a comunicação de dados, ou seja, no caso, a apreensão (por ordem judicial) da base física com os dados não se confunde com a quebra do sigilo ou interceptação das comunicações (BRASIL, 2006). Mais tarde, no já mencionado HC n° 91.867, a Segunda Turma do STF, na relatoria do ministro Gilmar Mendes, aplicou o mesmo entendimento para afirmar que o acesso policial ao registro de chamadas no celular de corréu, executor de crime, não representa violação do Art. 5º, XII da CF que não poderia ser interpretado de modo a proteger os dados armazenados (registro telefônico), uma vez que o dispositivo constitucional daria guarida apenas à comunicação de dados, no caso, a telefônica² (BRASIL, 2012). É imperioso destacar que o passar do tempo somado ao expressivo avanço tecnológico tornou obsoleta essa leitura constitucional da Suprema Corte.

Em síntese, o que se observa é que o próprio STF, em decisões posteriores, viu-se incumbido a tutelar situações em que o objeto da proteção eram os dados pessoais em si mesmos. Um caso de grande magnitude pela sua repercussão e importância foi o julgamento da ADI n° 6387 e outras³, que invalidou a medida provisória (MP) 954, de 17 de abril de 2020, em que a presidência da República autorizava “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” (Art. 1º) para subsidiar as estatísticas oficiais, durante a pandemia do novo coronavírus, permitindo a realização de entrevistas

¹ Queiroz e Ponce (2020), destacam, contudo, que o STF incorporou seletivamente a tese do professor Tércio Sampaio.

² Ao analisar os julgados mais recentes do STJ, Muniz (2021) concluiu que são tidas como ilícitas as provas obtidas do celular do preso como SMS e ‘Whatsapp’ quando acesso se dá sem ordem judicial, contudo o acesso não será ilícito quando baseado exclusivamente na agenda de contatos ou registros telefônicos, seguindo o entendimento de que a CF protege a comunicação telefônica e não os dados armazenados. O tema está pendente de julgamento no STF no ARE n° 1042075 (tema 977 da repercussão geral).

³ As demais ações foram as ADIs: 6388; 6389; 6390 e 6393.

em caráter não presencial, no âmbito de pesquisas domiciliares. A MP incidia no compartilhamento eletrônico da “relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas” (Art. 2º), sendo que após o ato do presidente do IBGE, os dados deveriam ser entregues no prazo de sete dias, contados a partir da publicação do mesmo ato (Art. 2º, § 3º, I). O grande alcance e a vagueza da MP fez com que o ato fosse contestado, por ADIs, pelo Conselho Federal da Ordem dos Advogados do Brasil (CFOAB), e por partidos políticos. Já em 24 de abril de 2020, a ministra Rosa Weber, do STF, suspendeu, liminarmente, a MP em comento.

Considerado o julgamento definitivo do mérito pelo pleno do STF, alguns dos pontos relevantes serão explorados neste trabalho. Com efeito, é interessante destacar que a tese jurídica é a proteção dos dados em si mesmos, para alcançar, prioritariamente, a proteção da pessoa, assim,

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 (BRASIL. SUPREMO TRIBUNAL FEDERAL. Pleno. Referendo na Medida cautelar na Ação Direta de Inconstitucionalidade 6.387-DF. Rel. Min. Rosa Weber. Julgamento em: 07 mai. 2020, p.2).

Na mesma oportunidade o Tribunal reconheceu que o respeito à privacidade e à autodeterminação informativa (Art. 2º, I e II da LGPD) são decorrência dos direitos da personalidade. Sobretudo, como os dados permitem a identificação (ainda que em potencial da pessoa), a falta de previsão de mecanismos de segurança da informação no texto da MP, acabaram por torná-la incapaz de atender as exigências constitucionais da proteção dos direitos fundamentais de mais de uma centena de milhão de brasileiros, usuários de telefonia, ali representados pelos seus dados, sem uma proteção adequada contra acessos não autorizados, vazamentos, utilização indevida e garantia da higidez, sigilo e anonimato dos dados. Além disso, o STF julgou que, mesmo diante da necessidade de estatísticas oficiais (no difícil cenário da pandemia da Covid-19), esse argumento não pode ser utilizado “visando ao enfraquecimento de direitos e atropelo de garantias fundamentais consagradas na Constituição” (BRASIL, 2020d, p.3).

Ademais, ao não definir, adequadamente, o tratamento e a finalidade para os quais os dados seriam utilizados, a MP hostilizou a garantia do devido processo legal (Art. 5º, LIV da CF), pelo fato de não oferecer “condições de avaliação quanto à sua adequação e necessidade, assim

entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades” (BRASIL, 2020d, p.2). Não restando outra conclusão que não fosse suspender a eficácia da medida provisória, para prevenir danos irreparáveis à intimidade e ao sigilo da vida privada dos milhões de usuários dos serviços de telefonia fixa e móvel.

A decisão do STF, no caso, recebeu expressivo apoio dos estudiosos que chegaram a afirmar que houve, de fato, o reconhecimento de um direito fundamental à proteção de dados pessoais (WIMMER, 2021a) e (MENDES; RODRIGUES JR.; FONSECA, 2021). Sob outro viés, é importante destacar ainda a preocupação do Tribunal com a finalidade para a qual tais dados seriam compartilhados. Mormente, a finalidade é um princípio insculpido na LGPD, que a define como “realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades” (Art. 6º, I da LGPD, grifo nosso). Não obstante, a vigência parcial da Lei seja de 2020, o próprio STF já foi acionado em anos anteriores para defender, de certo modo, a finalidade da coleta de dados. São ilustrativas, portanto, as medidas cautelares nos casos da suspensão de liminar 1.103/2017-SP e do MS nº 36.150/2018-DF. No primeiro caso, a ministra Cármen Lúcia entendeu pela impossibilidade do compartilhamento de dados de recenseamento do IBGE com o Ministério Público Federal (MPF), por entender que aqueles dados sigilosos de 45 crianças não registradas em cartório foram obtidos com a finalidade específica de produção da estatística oficial, razão pela qual o compartilhamento com o MPF ameaçava a confiança dos entrevistados no IBGE, atraindo o risco de que informações inverídicas passassem a ser descritas pelos entrevistados, minando a confiança das pesquisas pelo simples receio de que a finalidade poderia ser outra, além da produção estatística (BRASIL, 2017).

Em outro aspecto, o MS 36.150/2018, da relatoria do ministro Roberto Barroso, impediu o compartilhamento de dados do Censo Escolar do Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP) com o Tribunal de Contas da União (TCU), porque entendeu-se que aqueles dados foram obtidos com uma finalidade certa e com garantia do sigilo. No mais, a entrega dos dados ao TCU quebraria a confiança daqueles que forneceram as informações ao INEP, restando incompatível o seu compartilhamento com o TCU para outra finalidade, a saber, a auditoria no programa Bolsa Família pelo Tribunal de Contas (BRASIL, 2018b).

Mesmo após isso, o STF, analisou casos de alta relevância que perpassaram pela finalidade do tratamento, casos em que o mesmo Estado, que deveria garantir e regular os direitos fundamentais, notadamente, a privacidade e a proteção de dados pessoais, passou a ser um agente de violação e excessos em potencial contra esses direitos (PESSOA, 2020). No ponto nodal, a exemplo, tem-se a ADI nº 6529/2020-DF, em que o pleno do STF, debruçou-se sobre o alcance da requisição de dados pela Agência Brasileira de Informações (ABIN) e deu interpretação conforme ao Art. 4º da Lei nº 9.883/1999 limitando a prerrogativa estatal nestes termos:

a) os órgãos componentes do Sistema Brasileiro de Inteligência somente podem fornecer dados e conhecimentos específicos à ABIN quando comprovado o interesse público da medida, afastada qualquer possibilidade de o fornecimento desses dados atender a interesses pessoais ou privados; b) toda e qualquer decisão de fornecimento desses dados deverá ser devida e formalmente motivada para eventual controle de legalidade pelo Poder Judiciário; c) mesmo quando presente o interesse público, os dados referentes às comunicações telefônicas ou dados sujeitos à reserva de jurisdição não podem ser compartilhados na forma do dispositivo, em razão daquela limitação, decorrente do respeito aos direitos fundamentais; d) nas hipóteses cabíveis de fornecimento de informações e dados à ABIN, são imprescindíveis procedimento formalmente instaurado e a existência de sistemas eletrônicos de segurança e registro de acesso, inclusive para efeito de responsabilização em caso de eventual omissão, desvio ou abuso (BRASIL. SUPREMO TRIBUNAL FEDERAL. Pleno. AÇÃO DIRETA DE INCONSTITUCIONALIDADE 6.529-DF. Rel. Min. Cármen Lúcia, Julgamento concluído em: 08 out. 2021).

A ADI, proposta pelo partido Rede Sustentabilidade e outros, quando ajuizada, pautou-se pelo receio do uso da estrutura de inteligência do Estado em desrespeito aos direitos e garantias fundamentais, constituindo-se em verdadeiro cenário de agigantamento dos riscos de abusos estatais sobre os cidadãos, ali representados pelas suas informações pessoais. A Suprema Corte, ainda em 2020, analisou outro caso semelhante: a Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 695 que trata do já extinto termo de autorização nº 7/2020 em que se previu o compartilhamento de dados constantes da Carteira Nacional de Habilitação (CNH), entre o SERPRO e a ABIN, com alcance sobre mais de 70 milhões de brasileiros. Em sede de medida cautelar o relator ministro Gilmar Mendes negou a perda de objeto da ação para assegurar a análise sobre a possível violação, em abstrato, das disposições do Decreto nº. 10.046/2019 contra o Art. 5º, caput, X e XII, da CF. Consignando a relevância da matéria, anotou que o regime jurídico incidente no compartilhamento de dados entre órgãos e instituições do Estado “é matéria de extrema relevância para a proteção constitucional do direito constitucional à privacidade (art. 5º, caput e

incisos X, da Constituição Federal), situando-se como garantia elementar de qualquer sociedade democrática contemporânea” (BRASIL, 2020c, p. 47, grifos no original).

Ato contínuo, vislumbrou-se, desde logo, uma atuação acertada do STF no controle do cumprimento dos deveres de proteção pelos demais órgãos estatais (proibindo excessos) somada à atuação para sanar a proteção ineficiente dos direitos, uma verdadeira competência do Poder Judiciário (SARLET, 2021).

Analisando, de outro lado, decisões dos demais Tribunais brasileiros, exsurge um caso interessante para exame à luz dos direitos fundamentais e do alcance do interesse público. Trata-se do MS cível nº 2073723-23.2020.8.26.0000, julgado pelo Tribunal de Justiça do Estado de São Paulo (TJSP), em 2020. Em síntese, o impetrante era um cidadão e o impetrado era o governador daquele Estado. O primeiro alegou, em apertada síntese, que o acordo entre o Instituto de Pesquisas Tecnológicas (IPT) e operadoras de telefonia, para rastrear e monitorar os fluxos de deslocamento durante a vigência da quarentena destinada ao combate da disseminação do novo coronavírus, violava à intimidade e a privacidade das pessoas titulares de contas telefônicas com seus dados e localização monitorados pelo Estado, na iminência de ordem de prisão arbitrária.

Instada a se manifestar a Administração Pública paulista esclareceu que não realizava o tratamento de nenhum dado pessoal, pois os dados tinham propósito meramente estatístico, e eram anonimizados, ou seja, era um “dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento” (Art. 5º, III da LGPD). Por apresentarem dados do dia anterior, e pelo fato de que o mecanismo de sistematização apenas possuía recursos de visualização de mapas e de gráficos de isolamento e de circulação, não era possível reverter o processo que tornava anônimos, inclusive quanto a operadora quanto ao detentor do dispositivo celular. Naquela oportunidade o TJSP denegou a ordem com o seguinte fundamento “assegurado o anonimato, preservado o sigilo dos dados apurados pelas empresas de telefonia móvel antes da transferência ao IPT, não há afronta a direito individual, inviabilizando o acolhimento da demanda” (SÃO PAULO, 2020, p. 9), nos termos do voto do relator. A prática paulista também foi contestada, sem sucesso, a exemplo, no HC nº 574.431/SP, relatoria da ministra Laurita Vaz, do STJ.

A intensificação do uso de tecnologias pelo Estado para combater ou mitigar os efeitos da pandemia (Covid-19) foi um instrumento essencial na gestão das políticas públicas, decorrência do dever de proteção do direito à saúde e à vida de todos. Daí, surgiu um impasse interessante, no

sentido de que estudos na área da administração pública se mostraram favoráveis à ampliação do tratamento de dados pelo governo para subsidiar as políticas públicas, ao contrário do que pensavam os estudos de vigilância que são mais críticos à prática (WIMMER, 2021a).

No caso do monitoramento de celulares, podia-se inferir que o tratamento foi feito com base em um interesse público, mas a administração, ainda que no cumprimento de dever legal, não podia ignorar os pressupostos da LGPD deixando os titulares de dados sempre bem informados sobre as condições do tratamento como base legal, finalidade, procedimentos e ciclo de vida (OLIVEIRA, 2020). De outra parte, mostrou-se perfeitamente legítimo o recurso ao Judiciário para que o cidadão pudesse garantir, se fosse o caso, o seu direito à autodeterminação informativa sobre seus dados, um direito oponível a terceiros (até mesmo o governo), ou seja, “abrangendo a potestade do indivíduo de perguntar, receber informação, limitar a circulação, opor-se, proibir e fazer cessar as informações daí derivadas” (PESSOA, 2020, p. 89). É um nítido sinal dos tempos em que a afronta à privacidade, à intimidade e à própria proteção de dados tem sido proporcional ao avanço tecnológico da comunicação, sobretudo, com informações pessoais transmitidas a terceiros sem autorização ou conhecimento do titular (MACHADO, 2018).

Outrossim, convém versar sobre um problema semelhante: quando o acesso à Justiça Trabalhista passa a ser um risco para o trabalhador, ainda que a publicidade processual seja um mandamento da Constituição. A problemática surgiu pelo fato de que a internet facilitou e massificou o acesso aos processos trabalhistas, de tal sorte os dados do trabalhador passaram a estar públicos no site dos Tribunais respectivos, ostentando o fácil acesso à transferência e à obtenção por bancos de dados, infelizmente, por vezes, para fins discriminatórios que dificultam a reinserção do trabalhador no mercado, as chamadas “listas sujas” de autores de reclamações trabalhistas.

É assente, contudo, que a publicidade processual também recai sobre as demandas trabalhistas sendo, portanto, um grande desafio separar a coleta de dados necessária à prestação jurisdicional, em contraposição àquilo que, realmente, deve, e como deve vir a público, sem expor, excessivamente, a informação privada. A controvérsia foi objeto do quinto “considerando” da resolução nº 121/2010, do Conselho Nacional de Justiça (CNJ) que afirma, expressamente, a existência de dificuldades no Judiciário pela “estigmatização” de autores ou réus em ações, inclusive trabalhistas. Sobremodo, a referida resolução estipulou quais dados podem ser utilizados para consultas públicas em ações trabalhistas.

Mais tarde sobreveio a resolução nº 139/2014, do Conselho Superior da Justiça do Trabalho (CSJT) que determinou aos Tribunais Regionais do Trabalho (TRTs) a adoção de medidas contra as “listas sujas”, dificultando a indexação de dados sensíveis em mecanismos de buscas, além de dificultar as capturas automáticas ou robôs de busca nos seus respectivos sites. Muito embora, ainda seja possível encontrar, segundo Lamberty (2020) vários dados de ações trabalhistas em buscadores apenas com o nome das partes, afrontando direitos do trabalhador. A complexidade da matéria chegou ao Supremo Tribunal Federal, e foi reconhecida a repercussão geral da questão constitucional apresentada no RE com agravo nº 1.307.386/2021-RS, no caso, em síntese, discute-se a constitucionalidade da divulgação, pelos sites, de nomes de pessoas vinculadas a processos judiciais, sem sigredo de justiça, facilitando a elaboração de “listas sujas” pelos empregadores, a exemplo. Trata-se de controvérsia relevante entre a intimidade dos indivíduos e a publicidade processual e os atos do próprio Judiciário, publicados nos diários oficiais.

3.2 Um Direito ao Esquecimento: entre o Protagonismo Judicial e o Silêncio Legislativo

O direito ao esquecimento também chamado de “direito a ser esquecido” (*right to be forgotten*) ou desindexação é uma das mais interessantes questões relacionadas ao Marco Civil da Internet, muito embora já existissem demandas judiciais, antes mesmo dessa Lei⁴. O direito ao esquecimento, ao que se depreende, não dá ao indivíduo o condão de reescrever ou impor um sigilo sobre o seu passado, ao contrário decorre da dignidade da pessoa humana somada ao fato de não ser sempre lembrado “pela força” da memória da internet e outros meios quase sempre muito acessíveis ao público, por acontecimentos pretéritos, que já não guardam relevância para com o presente. Como anotou Martins (2020) há uma complexa oposição de interesses, pois:

o direito ao esquecimento se insere em um delicado conflito de interesses. De um lado, o interesse público aponta no sentido de que fatos passados sejam lembrados, considerando ainda a liberdade de imprensa e de expressão, bem como o direito da coletividade à informação; do outro, há o direito de não ser perseguido por toda a vida por acontecimento pretérito (MARTINS, 2020, p. 5).

⁴ A propósito, veja-se o Recurso Especial nº 1.316.921-RJ, julgado em 2012, envolvendo uma conhecida personalidade da Tv brasileira.

Diferentemente do GDPR europeu que prevê, expressamente, o direito ao apagamento no seu Art. 17, o Brasil não possui norma expressa sobre o tema. O MCI estabeleceu ao Poder Judiciário a prerrogativa da remoção, bloqueio ou exclusão de conteúdos infringentes a direitos na internet, ou seja, trata-se de uma reserva de jurisdição em atenção à liberdade de expressão e a vedação à censura (Art. 19 do MCI). Nesse ponto, há o Recurso Especial (REsp) nº 1.342.640/2017-SP, que reconheceu a impossibilidade de que o provedor de pesquisa (Google) realizasse controle prévio de buscas para impedir a exibição de dados pessoais constantes na extinta rede social Orkut. O julgado também destacou que compete ao responsável pelo site a remoção de conteúdo ilícito, tão logo tome conhecimento inequívoco, sob pena de responsabilização ulterior. Note-se que a ação foi ajuizada, inicialmente, no ano de 2008.

Outra controvérsia mais ilustrativa foi o REsp nº 1.660.168/2018-RJ, que tratou de equilibrar o interesse da autora (membro do Ministério Público) pela desindexação de seu nome dos resultados de busca que tratavam de fraude (posteriormente não comprovada) em concurso da magistratura, pretensão a ser sopesada com o interesse coletivo de acesso aos conteúdos noticiados, mesmo que passada mais de década do ocorrido. A Terceira Turma do STJ, por maioria, entendeu que a circunstância específica exigia do Judiciário uma atuação para que a pesquisa (exclusiva) pelo nome da autora não indexasse o fato noticiado, permitindo, contudo, a consulta a quem procurasse pelo fato noticiado em si. Ademais, enfatizou-se que a busca pela informação privada (o nome), somada ao passar dos anos faz com que não seja mais relevante para o interesse público a mera indexação do nome do indivíduo protegido. Ficou assim assentado:

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 (BRASIL. SUPERIOR TRIBUNAL DE JUSTIÇA. Terceira Turma. RECURSO ESPECIAL Nº 1.660.168 - RJ. Rel. p/ acórdão Min. Marco Aurélio Bellizze. Julgado em: 08 mai. 2018, p. 1).

Como anotou Cueva (2021), o julgado supracitado não passou despercebido pela crítica pois mesmo que as informações noticiadas não eram inverídicas ou ofensivas, a Terceira Turma deu interpretação diversa daquela que vinha sendo dada ao MCI (Art. 19), quando se entendia que o provedor de pesquisa não poderia ser obrigado a eliminar de seus resultados certos termos ou expressões em conteúdo gerado por terceiros, uma vez que o MCI exige que a remoção judicial

desse tipo de conteúdo não possa ser abstrata, e sim com identificação específica e localização inequívoca do conteúdo. Além disso, por ter sido o fato noticiado já investigado pelo CNJ, e que a autora é pessoa em cargo relevante (membro do Ministério Público), o interesse da sociedade à informação deveria ter seu peso significativo considerado (CUEVA, 2021).

Mais tarde, em fevereiro de 2021, sobreveio a decisão do Supremo Tribunal Federal que envolveu a família de Aída Curi contra a Tv Globo, que havia reconstituído o assassinato da jovem Aída, ocorrido em 1958. O Tribunal afirmou que, em tese, é incompatível o direito ao esquecimento com a ordem constitucional vigente, devendo os eventuais abusos ou excessos em desfavor dos direitos de um indivíduo serem analisados, caso a caso. Com efeito, fixou-se a seguinte tese com repercussão geral:

é incompatível com a Constituição a ideia de um direito ao esquecimento, assim entendido como o poder de obstar, em razão da passagem do tempo, a divulgação de fatos ou dados verídicos e lícitamente obtidos e publicados em meios de comunicação social analógicos ou digitais. Eventuais excessos ou abusos no exercício da liberdade de expressão e de informação devem ser analisados caso a caso, a partir dos parâmetros constitucionais - especialmente os relativos à proteção da honra, da imagem, da privacidade e da personalidade em geral - e das expressas e específicas previsões legais nos âmbitos penal e cível (BRASIL. SUPREMO TRIBUNAL FEDERAL. Pleno. Recurso Extraordinário Nº 1.010.606-RJ. Rel. Min. Dias Toffoli. Julgamento em: 11 fev. 2021, p. 3-4).

Embora a LGPD tenha se inspirado no GDPR europeu, não previu um direito ao esquecimento. De outra parte, o silêncio do legislador sobre o tema pode indicar uma espera prudente sobre o reconhecimento desse direito, quiçá, aguardando seu delinear e seu alcance pelos Tribunais, e os estudiosos, além da compatibilidade desse direito com o notável desenvolvimento da tecnologia (CUEVA, 2021).

Ademais, percebe-se que o “direito ao esquecimento” é um tema complexo e que, por vezes, entra em colisão com outros direitos da vida em sociedade. O equilíbrio entre os interesses envolvidos, indubitavelmente, atrai o sopesamento à aplicação dos direitos pelo Judiciário.

4 Conclusão

O presente estudo concentrou-se na análise da importância e no papel do Poder Judiciário no reconhecimento e concretização do direito à proteção de dados pessoais e correlatos. Considerando que o surgimento de um direito fundamental individual independe da sua previsão

expressa no texto constitucional, evidencia-se o caráter meramente exemplificativo do rol previsto na Lei Maior, de tal sorte que o advento do inciso LXXIX, Art. 5º da CF (EC nº 115/2022), apenas ratificou aquilo que hodiernamente já vinha sendo reconhecido nos Tribunais, especialmente, o STF.

Com o desenvolver da pesquisa percebeu-se que a nova configuração mundial, repleta de computadores, de comunicações instantâneas, big data e todo o ostensivo avanço tecnológico que amoldam o atual sistema capitalista, acabam, todos eles, por trazer implicações aos direitos da personalidade. Essas implicações estão sintetizadas na experiência das últimas décadas, nos debates globais sobre a privacidade, a intimidade e, mais recentemente, a um direito à proteção dos dados pessoais.

Diante desse cenário, este estudo, delimitado ao caso brasileiro, deduziu que a rapidez com que a tecnologia impactou a vida das pessoas em geral exigiu, notadamente, do Poder Judiciário, uma resposta às demandas concretas em defesa da privacidade, da intimidade e, sobretudo, da proteção de dados pessoais, inclusive diante de potencial arbítrio do Estado. Trata-se de uma atuação iniciada ainda quando o ordenamento jurídico e a interpretação constitucional sobre o tema ainda não possuíam “precedentes” e, no mais, eram tomados por uma vagueza normativa e uma doutrina muito abstrata para um cenário tecnológico que se reinventa a cada dia. É fato que, posteriormente, com o advento do Marco Civil da Internet e da Lei Geral de Proteção de Dados Pessoais, o ordenamento brasileiro tornou-se mais completo e com paradigmas oponíveis ao Estado, ao setor privado e as pessoas em geral. Ainda assim, a missão do Judiciário, como um garantidor dos direitos envolvidos, subsiste com muita força. Tal asserção também se justifica pelo fato de que o direito positivo dificilmente consegue acompanhar a rapidez das mudanças da sociedade, conseqüentemente, o Juiz é chamado a pronunciar-se sobre os conflitos entre os jurisdicionados, muitas vezes, antes do próprio Legislador.

De qualquer modo, o alçar do direito à proteção de dados pessoais e correlatos não fazem deles direitos absolutos e, portanto, eles limitam-se com os naturais e variáveis conflitos atrelados aos deveres do Estado, aos particulares e ao próprio direito vigente como o princípio da publicidade. Se onde há sociedade há Direito, onde há pessoa que alega ter um direito seu, ignorado ou violado, há de haver magistrados para solucionar esses conflitos. Não se ignora que a vida em sociedade não permite a ninguém estar sob o anonimato completo, e nem ter os seus direitos de personalidade e sua dignidade vilipendiados pelo massivo alcance do processamento de dados pessoais. Daí,

Ciências Sociais Aplicadas em Revista, v. 28, n. 48, p. 356-380, Edição Especial, 2024.

depreende-se, nesta era da informação, que o público e o privado não se excluem um ao outro, e precisam conviver, mutuamente, em um equilíbrio regulado, caso a caso.

E é pelo direito brasileiro vigente que se depreende que esse “equilíbrio regulado” é definido, ainda que não exclusivamente, mas em última instância, pelo Judiciário a quem cabe tutelar, adequar e garantir os direitos fundamentais do cidadão, tal como consagrado na expressão do moleiro “ainda existem juízes em Berlim”.

Ante o exposto, a pesquisa concluiu que é satisfatória a proteção dada pelo Judiciário aos dados pessoais. A força normativa da Constituição restou hígida, mesmo em um cenário prepositivação do direito fundamental à proteção de dados pessoais (EC nº 115/2022). Por evidente, percebeu-se que essa proteção ainda está sendo desenvolvida e implementada no contexto social.

Referências

ANDRIEUX, François. **Le meunier de Sans-souci**. Disponível em: <<https://fdmf.fr/le-meunier-sans-souci/>>. Acesso em: set. 2021.

BBC NEWS. Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. **BBC News**. 20 de mar. de 2018. Disponível em: <<https://www.bbc.com/portuguese/internacional-43461751>>. Acesso em: setembro de 2021.

BRASIL. CONSELHO NACIONAL DE JUSTIÇA. **Resolução nº 121 de 05/10/2010**. CNJ. Acesso em: out. 2021.

BRASIL. CONSELHO SUPERIOR DA JUSTIÇA DO TRABALHO. **Resolução n. 139/CSJT, de 24 de junho de 2014**. Acesso em: out. 2021.

BRASIL. **Constituição Federal de 1988**. Planalto. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: out. 2021.

BRASIL. **Lei nº 12.965 de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Planalto. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>. Acesso em: out. 2021.

BRASIL. **Lei nº 13.709 de 2018**. Lei Geral de Proteção de Dados Pessoais. Planalto. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm>. Acesso em: out. 2021.

BRASIL. **Medida Provisória Nº 954, de 17 de abril de 2020**. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico [...]. Planalto.

Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm>. Acesso em: out. 2021.

BRASIL. SUPERIOR TRIBUNAL DE JUSTIÇA. Terceira Turma. **RECURSO ESPECIAL Nº 1.342.640 – SP**. Rel. Min. Nancy Andrighi. Julgado em: 07/02/2017. Acesso em: set. 2021.

BRASIL. SUPERIOR TRIBUNAL DE JUSTIÇA. Terceira Turma. **RECURSO ESPECIAL Nº 1.660.168 - RJ**. Rel. p/ acórdão Min. Marco Aurélio Bellizze. Julgado em: 08/05/2018. Acesso em: set. 2021.

BRASIL. SUPREMO TRIBUNAL FEDERAL. Pleno. **AÇÃO DIRETA DE INCONSTITUCIONALIDADE 6.529-DISTRITO FEDERAL**. Julgamento concluído em: 08/10/2021. Rel. Min. Cármen Lúcia. Disponível em: < <http://portal.stf.jus.br/processos/downloadTexto.asp?id=5431804&ext=RTF>>. Acesso em: out. 2021e.

BRASIL. SUPREMO TRIBUNAL FEDERAL. Segunda Turma. **HABEAS CORPUS 91.867-PARÁ**. Julgamento em: 24/04/2012. Rel. Min. Gilmar Mendes. Acesso em: set. 2021.

BRASIL. SUPREMO TRIBUNAL FEDERAL. **MEDIDA CAUTELAR NA ARGUIÇÃO DE DESCUMPRIMENTO DE PRECEITO FUNDAMENTAL 695-DISTRITO FEDERAL**. Decidido em: 24/06/2020. Rel. Min. Gilmar Mendes. Acesso em: set. 2021c.

BRASIL. SUPREMO TRIBUNAL FEDERAL. **MEDIDA CAUTELAR EM MANDADO DE SEGURANÇA 36.150-DISTRITO FEDERAL**. Decidido em: 10/12/2018. Rel. Min. Roberto Barroso. Acesso em: set. 2021b.

BRASIL. SUPREMO TRIBUNAL FEDERAL. Presidência. **MEDIDA CAUTELAR NA SUSPENSÃO DE LIMINAR 1.103-SÃO PAULO**. Decidido em: 02/05/2017. Min. Cármen Lúcia. Acesso em: set. 2021.

BRASIL. SUPREMO TRIBUNAL FEDERAL. Pleno. **RECURSO EXTRAORDINÁRIO 418.416-SANTA CATARINA**. Julgamento em: 10/05/2016. Rel. Min. Sepúlveda Pertence. Acesso em: set. 2021.

BRASIL. SUPREMO TRIBUNAL FEDERAL. Pleno. **RECURSO EXTRAORDINÁRIO 673.707-MINAS GERAIS**. Julgamento em: 17/05/2015. Rel. Min. Luiz Fux. Acesso em: set. 2021.

BRASIL. SUPREMO TRIBUNAL FEDERAL. Pleno. **RECURSO EXTRAORDINÁRIO 1.010.606-RIO DE JANEIRO**. Julgamento em: 11/02/2021. Rel. Min. Dias Toffoli. Acesso em: set. 2021f.

BRASIL. SUPREMO TRIBUNAL FEDERAL. Pleno. **REPERCUSSÃO GERAL NO RECURSO EXTRAORDINÁRIO COM AGRAVO 1.307.386-RIO GRANDE DO SUL**. Julgamento em: 06/05/2021. Rel. Min. Luiz Fux. Acesso em: set. 2021g.

BRASIL. SUPREMO TRIBUNAL FEDERAL. Pleno. **REFERENDO NA MEDIDA CAUTELAR NA AÇÃO DIRETA DE INCONSTITUCIONALIDADE 6.387-DISTRITO FEDERAL**. Julgamento em: 07/05/2020. Rel. Min. Rosa Weber. Acesso em: set. 2021d.

CASTELLS, Manuel. **A sociedade em rede**. Tradução de: Roneide V. Majer. 6. ed. São Paulo: Paz e Terra, 1999.

CUEVA, Ricardo V. B. Proteção de dados pessoais e direito ao esquecimento. *In: Tratado de Proteção de dados pessoais*. (coord). DONEDA, D.; SARLET, Ingo W.; MENDES, Laura S.; RODRIGUES JR, Otavio L. 2ª reimpressão. Rio de Janeiro: Forense, 2021.

DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. *In: Tratado de Proteção de dados pessoais*. (coord). DONEDA, D.; SARLET, Ingo W.; MENDES, Laura S.; RODRIGUES JR, Otavio L. 2ª reimpressão. Rio de Janeiro: Forense, 2021.

FERRAZ JÚNIOR, Tércio. S. (1993). Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito**, Universidade de São Paulo, 88, pp. 439-459.

LAMBERTY, Andrey O. **Autodeterminação informativa no âmbito da Justiça do Trabalho: a proteção jurídica de dados pessoais do trabalhador em perspectiva comparada entre Brasil e Argentina**. Porto Alegre: Editora Fi, 2020.

MACHADO, Joana de M. S. **A tutela da privacidade na sociedade da informação: a proteção dos dados pessoais no Brasil**. Porto Alegre: Editora Fi, 2018.

MARTINS, Guilherme Magalhães. Direito ao esquecimento na era da memória e da tecnologia. **Revista dos Tribunais** [Recurso Eletrônico]. São Paulo, n.1019, set. 2020. Disponível em: <<https://www.thomsonreuters.com.br/content/dam/openweb/documents/pdf/Brazil/revistas-especializadas/rt-1019-guilherme-magalhaes-martins-direito-ao-esquecimento-na-era-da-memoria-e-tecnologia.pdf>>. Acesso em: out. 2021.

MARTINS, Marcelo G.; TATEOKI, Victor A. Proteção de dados pessoais e democracia: fake news, manipulação do eleitor e o caso da Cambridge Analytica. **Revista Eletrônica e Sociedade**, v. 7, n. 3, 2019. ISSN 2318-8081. Disponível em: <<https://revistas.unilasalle.edu.br/index.php/redes/article/view/5610>>. Acesso em: set. 2021.

MAXIMILIANO, Carlos. **Hermenêutica e aplicação do Direito**. 19. ed. Rio de Janeiro: Forense, 2003.

MENDES, Laura. S.; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei geral de Proteção de Dados. **Revista de Direito do Consumidor**, São Paulo, v. 120. Ano 27. p. 469-483, nov. dez. 2018.

MENDES, Laura S. A encruzilhada da proteção de dados no Brasil e o caso do IBGE. **Jota**. 23/04/2020. Disponível em: <<https://www.jota.info/opiniao-e-analise/artigos/a-encruzilhada-da-protecao-de-dados-no-brasil-e-o-caso-do-ibge-23042020>>. Acesso em: set. 2021.

MENDES, Laura S.; RODRIGUES JR, Otavio L.; FONSECA, Gabriel C. S. O Supremo Tribunal Federal e a proteção constitucional dos dados pessoais: rumo a um direito fundamental autônomo. *In: Tratado de Proteção de dados pessoais*. (coord). DONEDA, D.; SARLET, Ingo W.; MENDES, Laura S.; RODRIGUES JR, Otavio L. 2ª reimpressão. Rio de Janeiro: Forense, 2021.

MONTEIRO, Renato L. Lei Geral de Proteção de Dados do Brasil: análise contextual detalhada. **Jota**. 14 de jul. de 2018. Disponível em: <<https://www.jota.info/opiniao-e-analise/columas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-analise-detalhada-14072018>>. Acesso em: setembro de 2021.

MUNIZ, Gina R. G. Acesso aos celulares dos presos pelos policiais: da licitude à ilicitude. Tribuna da defensoria. **Conjur**. 02 fev. 2021. Disponível: <https://www.conjur.com.br/2021-fev-02/tribuna-defensoria-acesso-aos-celulares-presos-pelos-policiais-licitude-ilicitude?impri_mir=1>. Acesso em set. 2021.

NOGUEIRA, Fernanda A. C. M.; FONSECA, Maurício. L. **O consentimento na Lei Geral de Proteção de Dados: autonomia privada e o consentimento livre, informado, específico e expresso**. *In: Lei Geral de Proteção de Dados: uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial*. (Org.) Bernardo Menicucci Grossi, p. 192-213. Porto Alegre: Editora Fi, 2020.

OLIVEIRA, Guilherme H. G. As bases legais para o tratamento de dados pessoais: muito além do consentimento. *In: Lei Geral de Proteção de Dados: uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial*. (Org.) Bernardo Menicucci Grossi, p. 192-213. Porto Alegre: Editora Fi, 2020.

PERILLI, Paulo R. G. **Proteção de dados, privacidade e o Marco Civil da Internet**. *In: Lei Geral de Proteção de Dados: uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial*. (Org.) Bernardo Menicucci Grossi, p. 192-213. Porto Alegre: Editora Fi, 2020.

PESSOA, João Pedro Seefeldt. **O efeito Orwell na sociedade em rede: cibersegurança, regime global de vigilância social e direito à privacidade no século XXI**. Porto Alegre: Editora Fi, 2020.

QUEIROZ, Rafael Mafei Rabelo; PONCE, Paula Pedigoni. **Tércio Sampaio Ferraz Júnior e Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado: o que permanece e o que deve ser reconsiderado**. *Internet & Sociedade*, São Paulo, n.1, v. 1, p. 64-90, 2020.

REAL ACADEMIA ESPAÑOLA. **Diccionario del español jurídico**. Big data. Disponível em: <<https://dej.rae.es/lema/big-data>>. Acesso em: outubro de 2020.

RUARO, Regina Linden; MOLINARO, Carlos Alberto. **Conflito real ou aparente de interesses entre o direito fundamental à proteção de dados pessoais e o livre mercado**. In: **Privacidade e proteção de dados pessoais na sociedade digital**. RUARO, Regina Linden; MAÑAS, José Luis P.; MOLINARO, Carlos A. (Org.). Porto Alegre: Editora Fi, 2017.

SÃO PAULO. TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO. Órgão Especial. **Mandado de Segurança Cível nº 2073723-23.2020.8.26.0000**. Julgamento em: 04/06/2020. Rel. Des. Evaristo Dos Santos. Acesso em: set. 2021.

SARLET, Ingo W. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: **Tratado de Proteção de dados pessoais**. (coord). DONEDA, D.; SARLET, Ingo W.; MENDES, Laura S.; RODRIGUES JR, Otavio L. 2ª reimpressão. Rio de Janeiro: Forense, 2021.

SARLET, Ingo W.; SAAVEDRA, Giovani A. Fundamentos jusfilosóficos e âmbito de proteção do direito fundamental à proteção de dados pessoais. **Direito Público**, [S.l.], v. 17, n. 93, jul. 2020. ISSN 2236-1766. Disponível em: <<https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/4315>>. Acesso em: 26 set. 2021.

SCHREIBER, Anderson. Responsabilidade Civil na Lei Geral de Proteção de Dados Pessoais. In: **Tratado de Proteção de dados pessoais**. (Coord). DONEDA, D.; SARLET, Ingo W.; MENDES, Laura S.; RODRIGUES JR, Otavio L. 2ª reimpressão. Rio de Janeiro: Forense, 2021.

SOUSA, Zilda A. G.; FRANCO, Igor da S. **Aplicação da Lei Geral de Proteção de Dados ao poder público**. In: **Lei Geral de Proteção de Dados: uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial**. (Org.) Bernardo Menicucci Grossi, p. 192-213. Porto Alegre: Editora Fi, 2020.

STEINER, Sylvia. In: **Um Dia Pela Democracia: Painel 3 - Democracia e Justiça**. Evento da ABDCONST. 17 nov. 2020. Disponível em: <https://youtu.be/gc_jmqmZzSI>. Acesso em: set. 2021.

THE ECONOMIST. The world's most valuable resource is no longer oil, but data. **The Economist**. 06 de maio de 2017. Disponível em: <<https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>>. Acesso em: setembro de 2021.

UNGER, Roberto Mangabeira. **Economia do conhecimento**. Tradução de: Leonardo Castro. São Paulo: Autonomia Literária, 2018.

VIANNA, José R. A. O JUDICIÁRIO E A EFETIVIDADE DOS DIREITOS HUMANOS. **Revista CEJ**, XXII n. 74, p. 61-71, jan./abr. 2018. Disponível em: <revistacej.cjf.jus.br/cej/index.php/revcej/article/view/2290>. Acesso em set. 2021.

WIMMER, Miriam. Limites e possibilidades para o uso secundário de dados pessoais no poder público: lições da pandemia. **Revista Brasileira de Políticas Públicas**, vol. 11, n. 1., pp. 122-142, 2021a.

WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo Poder Público. *In: Tratado de Proteção de dados pessoais*. (coord). DONEDA, D.; SARLET, Ingo W.; MENDES, Laura S.; RODRIGUES JR, Otavio L. 2ª reimpressão. Rio de Janeiro: Forense, 2021b.