Bruno Barata
Laryssa Almeida
Leandro Frota
(Coordenadores)

ENSAIOS SOBRE A TRANSFORMAÇÃO DIGITAL NO DIREITO

Estudos em Homenagem ao Ministro Kássio Nunes Marques

OAB Editora
NACIONAL
Brasília – DF, 2021

Conselho Federal, 2021
Setor de Autarquias Sul - Quadra 5, Lote 1, Bloco M
Brasília – DF CEP: 70070-939

Distribuição: Conselho Federal da OAB – GRE
E-mail: oabeditora@oab.org.br

O Conselho Federal da OAB – por meio da OAB Editora – ressalta que as opiniões emitidas nesta publicação, em seu inteiro teor, são de responsabilidade dos seus autores.

Dados Internacionais de Catalogação na Publicação (CIP)
(Conselho Federal da Ordem dos Advogados do Brasil – Biblioteca Arx Tourinho)

E59

Ensaios sobre a transformação digital no direito : estudos em homenagem ao ministro Kássio Nunes Marques / coordenador: Bruno Barata, Laryssa Almeida, Leandro Frota – Brasília: OAB Editora, 2021.

xvi, 648 p.

34:004.738.5(81)
E59e

ISBN: 978-65-5819-016-5.

Nota de capa: "Apresentação: Felipe Santa Cruz".

1. Poder judiciário, inovação tecnológica, administração, doutrinas e controvérsias, Brasil. 2. Acesso à justiça, modernização, Brasil. 3. Processo eletrônico, utilização, resultado, Brasil. 4. Processo eletrônico, Brasil. 5. Serviço público, modernização, Brasil. I. Barata, Bruno, coord. II. Almeida, Laryssa, coord. III. Frota, Leandro, coord. IV. Nunes Marques, Kássio, 1972-. V. Conselho Nacional de Justiça (Brasil). VI. Título.

CDD: 341.256
CDU: 342.56 (81+410.1)

SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS COMO PRESSUPOSTOS PARA O PODER JUDICIÁRIO NA ERA DIGITAL: uma análise da Resolução CNJ 361/2020 e da Resolução STF 724/2020

Luiz Fux*
Gabriel Campos Soares da Fonseca*

1 INTRODUÇÃO

Há uma convergência quase uníssona no sentido de que os dados pessoais, atualmente, consistem em elemento central para as dinâmicas políticas e culturais da "sociedade da informação" [1] e para a circulação de bens e de serviços na dita "economia digital".

No imaginário popular, ecoado também pela imprensa, por empresários e por certas instituições governamentais, essa assertiva tem sido representada por meio de frases sobre a potencialidade dos dados pessoais como *insumos* ou *ativos* para a atividade econômica: os dados pessoais são *o novo petróleo* para a economia global ou o capitalismo contemporâneo é *movido a dados* (*data-driven*).[2] Como bem ressalta a cientista social holandesa, Johanna ("José") van

* Presidente do Supremo Tribunal Federal (STF) e do Conselho Nacional de Justiça (CNJ). Ex-Presidente do Tribunal Superior Eleitoral. Professor Titular de Processo Civil da Faculdade de Direito da Universidade do Estado do Rio de Janeiro (UERJ). Doutor e Livre Docente em Direito Processual Civil pela Universidade do Estado do Rio de Janeiro (UERJ). Membro da Academia Brasileira de Letras Jurídicas. Membro da Academia Brasileira de Filosofia.

* Assessor Especial da Presidência do Supremo Tribunal Federal (Secretaria-Geral da Presidência do STF). Coordenador do Comitê Executivo de Proteção de Dados (CEPD) do STF. Coordenador de Inovação do Centro de Direito, Internet e Sociedade do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (CEDIS/IDP). Mestrando em Direito Econômico, Financeiro e Tributário (subárea Direito Econômico e Economia Política) pela Universidade de São Paulo (USP). Bacharel em Direito pela Universidade de Brasília (UnB).

[1] Sobre as novas técnicas de processamento de dados e os seus riscos para os direitos de personalidade na sociedade da informação, confira-se o seminal trabalho do professor alemão Spiros Simitis: SIMITIS, Spiros. Reviewing privacy in an information society. **University of Pennsylvania Law Review**, v. 135, p. 707-746, 1987.

[2] Nesse sentido, confira-se: JULIO, Rennan A. "Dados são o novo petróleo" diz CEO da Mastercard – exceto por um pequeno detalhe. **Época Negócios**, 05 de julho de 2019.

Dijck, tanto para os efeitos negativos quanto para os efeitos positivos desse fenômeno, é bem verdade que há um certo fetichismo ideológico e alguns exageros nessas narrativas sobre o tema[3]. No entanto, é difícil ignorar os impactos estruturais na vida contemporânea que o profundo desenvolvimento de campos como telecomunicações, computação e microeletrônica.

Com a difusão de tecnologias como os *smartphones*, o incremento do acesso à Internet principalmente em países do "Norte Global"[4] e a proliferação do uso de redes sociais pela população, cada vez mais relações cotidianas se tornaram "alvo" de grandes empresas de tecnologia e de publicidade digital, com o objetivo de extrair valor político-econômico desse "*material cru*", os dados pessoais.[5] Assim, a monetização dos dados pessoais se tornou uma realidade inexorável tanto no *âmbito privado*, por exemplo, no tocante à publicidade direcionada para oferecimento de bens e de serviços personalizados; quanto no *âmbito público*, com o ímpeto do Estado em tomar decisões empiricamente informadas e em desenvolver políticas públicas dotadas de maior eficiência.

Em apertada síntese, trata-se de cenário de onipresença tecnológica e de *ubiquidade computacional*, no qual equipamentos eletrônicos são parte constitutiva da rotina de vários cidadãos e em que os meios de comunicação pessoal foram remodelados.[6] Em grande parte, tal cenário está relacionado com o potencial que as informações extraídas desses dados podem oferecer como subsídio para inferências, interpretações, ranqueamentos, perfilizações e

---

Disponível em: https://epocanegocios.globo.com/Empresa/noticia/2019/07/dados-sao-o-novo-petroleo-diz-ceo-da-mastercard.html. Acesso em: 05 fev. 2021.

[3] Para sua análise crítica desse fenômeno, confira-se.: VAN DIJCK, Johana. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. **Surveillance & Society**, v. 12, n. 2, p. 197-208, 2014.

[4] Valendo-se dessa nomenclatura (Global North/Global South), analisando o livro de Daniel Bonilla Maldonado, vide: GARGARELLA, Roberto. Constitutionalism of the Global South. **International Journal of Constitutional Law**, v. 15, issue 2, p. 571-573, April 2007.

[5] BIONI, Bruno R.; ZANATTA, Rafael A. F. **Direito e economia política dos dados**: um guia introdutório. *In*: DOWBOR, Ladislau (org.). **Sociedade Vigiada**: como a invasão da privacidade por grandes corporações e Estados autoritários ameaça instalar uma nova distopia. São Paulo: Autonomia Literária, 2020.

[6] MENDES, Laura Schertel. Proteção de dados pessoais: fundamento, conceitos e modelo de aplicação. **Panorama setorial da Internet**, ano 11, n. 2, p. 1-7, junho de 2019, p. 1.

predições sobre indivíduos e grupos sociais em áreas fundamentais da vida (*v.g.* acesso ao crédito e a seguros; mercado de trabalho; eleições etc.).[7]

Ocorre que, se por um lado, esse potencial pode ser aproveitado de forma altamente benéfica para o surgimento de tecnologias inovadoras e para a formulação de políticas públicas mais eficientes. Por outro lado, inevitavelmente ele carrega consigo riscos de vigilância e de monitoramento social tanto por corporações, quanto por governos, bem como manipulações eleitorais, ataques *crackers*[8] de caráter maléfico, *discriminações algorítmicas*[9] ilegítimas e vazamentos de dados pessoais.

Nessa linha, o presente ensaio possui o *objetivo geral* de explorar esse contexto ambivalente de ebulição tecnológica e de transformação social. No entanto, detém o *objetivo específico* de avaliar seus impactos no âmbito das atividades do Poder Judiciário. O *recorte da investigação* aqui proposta elegeu o Conselho Nacional de Justiça (CNJ) e o Supremo Tribunal Federal (STF) como *objetos de análise*, uma vez que (a) são as duas instituições centrais na atividade de coordenação nacional dos esforços de gestão dos Tribunais e (b) possuem a pretensão de, respectivamente, introduzir um "*Juízo 100% Digital*" e fixar uma "*Corte Constitucional Digital*".

Além desta introdução e da conclusão, o desenvolvimento do texto realiza uma *descrição analítica* de normativas editadas pelas instituições supracitadas, relacionadas à segurança da informação e à proteção de dados no Poder Judiciário nacional. A *primeira parte* do ensaio aborda a Resolução CNJ 361/2020, que dispõe sobre o *Protocolo de Prevenção a Incidentes Cibernéticos no âmbito do Poder Judiciário* (PPICiber/PJ) estabelecido pelo Comitê de Segurança Cibernética do Poder Judiciário (Portarias CNJ 242/2020 e 249/2020). Por sua vez, a *segunda parte* trata da Resolução STF 724/2020, que instituiu o Comitê Executivo de Proteção de Dados (CEPD) para adequar

---

[7] MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **Revista Estudos Institucionais**, Rio de Janeiro, v. 6, n. 2, p. 507-533, maio/ago. 2020, p. 517-519.

[8] Sobre o desenvolvimento da "cultura hacker" e sua diferenciação com os ataques maléficos destinados a derrubar sistemas informacionais e corromper serviços digitais, confira-se: SILVEIRA, Sérgio Amadeu. Ciberativismo, cultura hacker e o individualismo colaborativo. **Revista USP**, v. 1, p. 28-39, 2010.

[9] Para uma tipologia das discriminações algorítmicas, confira-se: MENDES, Laura Schertel; MATTIUZO, Marcela. Discriminação Algorítmica: conceito, fundamento legal e tipologia. **Revista de Direito Público**, Porto Alegre, v. 16, n. 90, p. 39-64, nov./dez. 2019.

o Supremo Tribunal Federal à Lei n. 13.709, de 14 de agosto de 2019 (Lei Geral de Proteção de Dados - LGPD).

2 O CONSELHO NACIONAL DE JUSTIÇA E O COMITÊ DE SEGURANÇA CIBERNÉTICA DO PODER JUDICIÁRIO

A segurança da informação é elemento crucial para concretamente assegurar a proteção dos dados pessoais dos usuários de sistemas informáticos. É que, em uma sociedade livre e democrática, a garantia do direito à *autodeterminação informativa*[10] dos cidadãos pressupõe, anteriormente, a *confidencialidade* e a *integridade* dos sistemas informáticos utilizados. Desse modo, por exemplo, é necessário proteger as informações pessoais dos usuários desse sistema contra violações, interceptações e manipulações de terceiros.

Vale mencionar que esse foi justamente o raciocínio adotado pelo Tribunal Constitucional alemão no julgamento de reclamação constitucional proposta contra dispositivos legais do Estado de Nordrhein-Westfalen, no âmbito do caso popularmente conhecido como *Computer-Grundrecht*, cujo acórdão foi capitaneado pelo eminente professor Wolfgang Hoffman-Riem.[11] No referido caso, a Corte Constitucional alemã extraiu um direito fundamental à garantia da confidencialidade e da integridade dos sistemas informáticos (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*) à luz dos direitos ao livre desenvolvimento da personalidade e à dignidade da pessoa humana (artigos 2, I, c/c Art. 1, I, da Lei Fundamental alemã).[12]

Não por outra razão, o Conselho Nacional de Justiça (CNJ) seguiu esse ímpeto e criou o *Comitê de Segurança Cibernética do Poder Judiciário* (CSCPJ), previsto nas Portarias CNJ nº 242/2020 e 249/2020, justamente para garantir a integridade e a confidencialidade dos sistemas do Poder Judiciário

[10] Sobre a criação e o desenvolvimento desse direito na jurisprudência do Tribunal Constitucional Federal alemão, vide: MENDES, Laura Schertel. Autodeterminação informativa: a história de um conceito. **Revista Pensar**, Fortaleza, v. 25, n. 3, 2020.

[11] Vide a apresentação de Laura Schertel Mendes em livro de autoria do referido Juiz: HOFFMANN-RIEM, Wolfgang. **Teoria Geral do Direito Digital**: transformação digital e desafios para o direito. Rio de Janeiro: Forense, 2021.

[12] MENKE, Fabiano. A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. **Revista Jurídica Luso-Brasileira**, ano 5, n. 1, p. 781-809, 2019, p. 793-800.

brasileiro por meio de um combate a ataques invasivos de terceiros e pela prevenção de incidentes cibernéticos.

Com base na competência do CNJ para coordenar o planejamento, a gestão estratégica e a governança das Tecnologias de Informação e de Comunicação (TICs) do Poder Judiciário brasileiro (Resolução CNJ nº 211/2015) e do Sistema de Segurança do Poder Judiciário (Resolução CNJ nº 176/2013), a criação do Comitê teve como objetivo central o estabelecimento de diretrizes gerais sobre os processos de trabalho e as boas práticas em segurança da informação judiciária, sobretudo por mediante a apresentação do *Protocolo de Prevenção a Incidentes Cibernéticos no âmbito do Poder Judiciário* (PPICiber/PJ).

Por óbvio, o caráter desse Protocolo é o de orientação. Sem substituir as políticas, os processos e os procedimentos internos dos diversos órgãos do Poder Judiciário brasileiro, o PPJCiber consiste em um plexo de diretrizes direcionadas à prevenção dos incidentes de segurança, à gestão do risco organizacional, ao enfrentamento das ameaças e dos ataques aos sistemas judiciários, assim como à reparação de eventuais danos causados. É que a eficiência da segurança da informação, no âmbito judicial, demanda um acompanhamento especializado do respectivo Tribunal na prevenção, na detecção, na triagem, na análise, na resposta e na contenção dos incidentes de segurança, bem como na recuperação de informações e na reparação de eventuais danos ocorridos. É dizer: o respectivo Tribunal deve incrementar a segurança de seus sistemas de acordo com os aprendizados incorporados em cada uma dessas fases e nas ocorrências vivenciadas.

O primeiro pilar desse arcabouço regulamentar é o da *repressão*, fomentando respostas tempestivas aos incidentes de segurança. Nos inevitáveis momentos de crise, a atuação do CSCPJ e a disponibilidade desse marco infra legal serão extremamente relevantes para auxiliar a atuação repressiva do Poder Judiciário em face de eventuais ataques cibernéticos ou incidentes internos de segurança. É dizer: combatendo-os com mecanismos de "contra-ataque" ou com medidas de apaziguamento dos danos, para que o funcionamento normal seja rapidamente reinstaurado e os responsáveis identificados.

Nesse pilar, medida de suma importância é a formalização de Equipes de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) com o fito de promover a solução adequada e tempestiva das demandas e dos incidentes. Essa

solução preferencialmente será formulada sob uma perspectiva multidisciplinar, por meio de equipe composta por membros da área de tecnologia da informação, do setor jurídico, do controle interno e da própria comunicação dos Tribunais, essa última com o intuito de manter os cidadãos cientes e informados das respostas elaboradas pela área técnica do órgão judicial a algum acontecimento.

No entanto, o segundo pilar é o da *prevenção*. Conforme salientado no acórdão de aprovação da Resolução CNJ 361/2020[13], essa meta de governança destaca a importância consolidada pelos princípios da segurança e da prevenção (artigo 6º, incisos VII e VIII, c/c 46 a 49, da LGPD). O *primeiro* concretizado pela "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão". Já o *segundo* a partir da "adoção de medidas para prevenir a ocorrência de danos em virtude" do tratamento de dados pessoais pelo próprio Tribunal e de acessos não autorizados ou situações acidentais e ilícitas geradas por terceiros.

Noutras palavras, a segurança da informação do Poder Judiciário necessita de uma otimização dos recursos humanos, financeiros e tecnológicos que está interligada não só com a repressão de ilícitos ou de acidentes, mas também com o estabelecimento de protocolos preventivos e o aperfeiçoamento constante de regras de "boas práticas". Tudo isso em conformidade com as disposições aplicáveis da Lei de Acesso à Informação (LAI), do Marco Civil da Internet (MCI) e da própria Lei Geral de Proteção de Dados Pessoais (LGPD).

Para tanto, a Resolução contém 4 (quatro) artigos. O artigo 1º da Resolução CNJ nº 361/2020 determina a obrigatoriedade de sua observância por todos os órgãos do Poder Judiciário, exceto o Supremo Tribunal Federal, os quais deverão adotar o referido Protocolo, procurando ainda contemplar as melhores práticas e metodologias de gestão de risco organizacional e de prevenção de incidentes cibernéticos.

O artigo 2º da Resolução CNJ 361/2020, por sua vez, assegura a necessária abertura e plasticidade do PPICiber/PJ. A sua atualização não se dará somente com a edição da Estratégia da Segurança Cibernética e da Informação do Poder Judiciário, também de competência do CSCPJ. Ao revés, os parâmetros

[13] Confira-se o voto condutor do Ministro Luiz Fux, proferido no Processo nº 0010158-46.2020.2.00.0000, 323ª Sessão Ordinária do Conselho Nacional de Justiça, em 15/12/2020, o qual guiou esta seção do texto.

estabelecidos poderão ser adaptados "a qualquer tempo, por meio de Portaria da Presidência do CNJ", em vista das rápidas mudanças inerentes ao tema regulamentado, tais como: o desenvolvimento de novas tecnologias, o surgimento de novas técnicas de ataques cibernéticos e o estabelecimento de novas recomendações acerca das boas práticas para segurança da informação em face de alterações nas duas circunstâncias anteriores.

Por fim, o artigo 3º da norma estipulou o prazo de 60 (sessenta) dias, contados da publicação do ato que instituiu o CSCPJ (Portaria CNJ 292/2020), para cada órgão do Poder Judiciário elaborar e formalizar um *plano de ação* indicativo de seu próprio PPICiber, enviando-o ao CNJ no intuito de garantir a segurança do ecossistema digital do Poder Judiciário nacional. Por força de seu 4° artigo, a Resolução não só revogou as disposições em contrário, bem como entrou em vigor na data de sua publicação.

3 O SUPREMO TRIBUNAL FEDERAL E O COMITÊ EXECUTIVO DE PROTEÇÃO DE DADOS PESSOAIS:

Apesar de o Supremo Tribunal Federal estar expressamente excluído do escopo de incidência da Resolução CNJ 361/2020, certamente a orientação da Suprema Corte brasileira deve ser compatível com as diretrizes propostas pelo CNJ. Afinal, ambos possuem um dever de articulação institucional: não só atuando como coordenadores do Poder Judiciário nacional, mas também se portando como *exemplo* para todos os órgãos jurisdicionais.

A recente Resolução STF nº 724, de 2 de março de 2021, que instituiu o Comitê Executivo de Proteção de Dados (CEPD), deve ser comemorada justamente por direcionar o Tribunal no sentido dessa sua missão institucional. Em linhas gerais, o seu objetivo é duplo: identificar e implementar as medidas cruciais para adequar o Supremo Tribunal Federal aos princípios e às exigências da Lei Geral de Proteção de Dados (LGPD - Lei n. 13.709, de 14 de agosto de 2019). Trata-se de portar-se como exemplo da própria Recomendação CNJ n° 73 que, apesar de não alcançar expressamente o STF, recomenda a todos os "órgãos do Poder Judiciário brasileiro a adoção de medidas preparatórias e ações inicias para adequação às disposições contidas na Lei Geral de Proteção de Dados – LGPD."

É que a crescente utilização de sistemas informacionais estruturados e da própria Internet por parte do Poder Judiciário brasileiro e pelos demais atores do Sistema de Justiça[14] deve se pautar pelos princípios da transparência e da publicidade (artigo 37, *caput*, da Constituição Federal) em conjunto com o imprescindível respeito ao direito à privacidade desses atores, bem como à sua autodeterminação informativa, ao seu livre desenvolvimento da personalidade, à dignidade e à inviolabilidade da intimidade, da honra e da imagem desses.

Ou seja, se a segurança da informação é uma condição desse processo de *digitalização* do Poder Judiciário (ao menos para a parcela dos atores do Sistema de Justiça que detém acesso à Internet e conexão à rede), a proteção de dados pessoais deve ser o pressuposto que norteia todo os procedimentos para tanto.

Em verdade, conforme reconhecido por vários votos proferidos pelo próprio Plenário do Supremo Tribunal Federal na ADIs 6.387 e correlatas, julgadas antes mesmo da entrada em vigor da LGPD, o Poder Público precisa sempre levar em consideração o direito fundamental à proteção de dados cuja *dimensão subjetiva* "se desdobra como liberdade negativa do cidadão oponível perante o Estado, demarcando seu espaço individual de não intervenção estatal". Porém, cuja *dimensão objetiva* também emanda uma "atuação estatal protetiva no sentido de estabelecer condições e procedimentos aptos a garantir o exercício e a fruição desse direito fundamental".[15]

Portanto, a Resolução STF nº 724/2021 deve ser lida dentro desse contexto de efetivação da tutela constitucional aos dados pessoais e de entrada em vigor da Lei Geral de Proteção de Dados. Nessa linha, o CEPD deverá avaliar os mecanismos de coleta, de armazenamento, de processamento e de tratamento de dados pessoais existentes no STF e propor ações voltadas ao seu aperfeiçoamento, com estratégias, políticas e metas concretas para que o STF se adeque à LGPD. Além disso, terá a incumbência de formular as diretrizes para a gestão de dados pessoais de acordo com a regulamentação aplicável,

---

[14] Conforme a cientista política, Maria Tereza Sadek, "*o sistema de justiça é mais amplo do que o poder judiciário* (...) [na medida em que envolve] *diferentes agentes: o advogado, pago ou dativo; o delegado de polícia; funcionários de cartório; o promotor público e, por fim, o juiz*" (SADEK, Maria Tereza Aina. O Sistema de Justiça. *In:* SADEK, Maria Tereza. (Org.). **O Sistema de Justiça**. Rio de Janeiro: Centro Edelstein de Pesquisas Sociais, 2010, p. 9-10).

[15] MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares da. STF reconhece direito fundamental à proteção de dados: comentários sobre o referendo da Medida Cautelar nas ADIs 687, 6388, 6389, 6390 e 6393. **Revista de Direito do Consumidor**, vol. 130/2020, p. 471-478, jul./ago. 2020.

bem como o dever de fiscalizar e supervisionar a execução dos planos, dos projetos e das ações aprovadas pelo próprio Comitê.

No entanto, essas atribuições serão executadas em coordenação (i) com o próprio Comitê Executivo de Segurança da Informação (CESI) do Tribunal, atualmente responsável pela modernização e pela adequação da política de segurança da informação do Tribunal às exigências da LGPD, assim como (ii) com as diversas unidades da Corte, as quais deverão prestar o auxílio necessário ao CEPD divulgando, promovendo e implementando as medidas estabelecidas. Na realidade, à semelhança do CSCPJ/CNJ, o CEPD preza por sua integração e por sua multidisciplinariedade, comportando composição que inclui representantes das mais diversas áreas do Tribunal e ainda valoriza a *expertise* "externa", sendo possível o convite de especialistas sobre temas específicos para auxiliar esse processo de adequação.

Segundo o artigo 3º da referida Resolução, além das atribuições já mencionadas, o grupo de trabalho será igualmente responsável por: (i) prestar orientações sobre o tratamento e a proteção de dados pessoais à luz das diretrizes estabelecidas na Lei 13.709, de 2018 e das demais normas internas da Corte; (ii) promover o intercâmbio de informações sobre a proteção de dados pessoais com outros órgãos e instituições, conferindo especial atenção ao relacionamento com a Autoridade Nacional de Proteção de Dados (ANPD); e (iii) criar uma verdadeira *cultura de proteção de dados* dentro do Tribunal, realizando eventos, organizando cursos e apresentando estudos para capacitar e para orientar os Ministros, os servidores, os colaboradores, os terceirizados e os estagiários do Tribunal, difundindo conhecimento especializado sobre a LGPD.

4 CONCLUSÃO

O presente ensaio refletiu sobre a necessidade de se adotar a segurança da informação e a proteção de dados pessoais como pressupostos do processo de "digitalização" das ferramentas de atuação e da rotina de trabalho do Poder Judiciário brasileiro, em linha com a iniciativa institucional *"Juízo 100% Digital"* (CNJ) e com o projeto de transformar o STF em uma *"Corte Constitucional Digital"*.

Desse modo, defendeu-se que o alcance de resultados frutíferos nesse processo de digitalização dos sistemas judiciários e das atividades

administrativo-jurisdicionais do CNJ e do STF demanda uma observância irrestrita da privacidade, da autodeterminação informativa e da proteção dos dados pessoais dos atores do Sistema de Justiça, garantindo-lhes previamente a confidencialidade e a integridade dos sistemas técnico-informacionais utilizados, com alto grau de segurança da informação.

Por conseguinte, *em primeiro lugar*, a Resolução n° 361/2020, do Conselho Nacional de Justiça, representa uma pioneira preocupação com a segurança da informação no Poder Judiciário, estabelecendo protocolos preventivos e ações repressivas importantes para incidentes cibernéticos sem, contudo, deixar de conferir certo grau de plasticidade a essas regras e a esses parâmetros. Essa medida é relevante justamente porque dá a dinamicidade necessária para adequá-los às mudanças sócio técnicas que poderão ocorrer.

Noutro giro, *em segundo lugar*, a posição institucional do Supremo Tribunal Federal impõe-lhe a responsabilidade de *dar o exemplo* ao Poder Judiciário. Nesse sentido, a Resolução STF n° 724/2021 é a concretização dessa missão no que diz respeito à obrigação de adequação de todos os órgãos jurisdicionais do país em se adequar à LGPD. Trata-se de importante iniciativa institucional do STF, pela qual o Comitê Executivo de Proteção de Dados (CEPD), em conjunto com o Comitê Executivo de Segurança da Informação (CESI), poderá desenvolver e implementar políticas internas sobre gestão de dados partindo do pressuposto de que (i) dados pessoais merecem proteção constitucional e de que (ii) os princípios da transparência e da publicidade no Judiciário só pode ser bem concretizados, caso estejam acompanhados de elevado respeito à autodeterminação informativa dos atores que compõem o Sistema de Justiça.

***

Por derradeiro, alterando a linguagem para um tom mais pessoal, gostaríamos de parabenizar os organizadores desta coletânea pela iniciativa de homenagear o eminente Ministro Kassio Nunes Marques. Não obstante, gostaríamos igualmente de congratular o próprio homenageado de forma efusiva. Ministro Nunes Marques, esta obra marca apenas o início de sua trajetória no Supremo Tribunal Federal, a qual certamente beneficiará o desenvolvimento da jurisdição constitucional brasileira. Em linha com o Ministro Celso de Mello, seu antecessor na cadeira da Suprema Corte brasileira, Vossa Excelência possui a

virtude republicana de mover-se sempre pela defesa intransigente dos direitos fundamentais e pela preservação do regime democrático.

REFERÊNCIAS

BIONI, Bruno R.; ZANATTA, Rafael A. F. Direito e economia política dos dados: um guia introdutório. *In:* DOWBOR, Ladislau (org.). **Sociedade Vigiada**: como a invasão da privacidade por grandes corporações e Estados autoritários ameaça instalar uma nova distopia. São Paulo: Autonomia Literária, 2020.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Portaria nº 242, de 10 de novembro de 2020**. Institui o Comitê de Segurança Cibernética do Poder Judiciário. DJe/CNJ nº 358/2020, p. 9-11, 11 nov. 2020.

_____. **Portaria nº 249, de 13 de novembro de 2020**. Designa os integrantes do Comitê de Segurança Cibernética do Poder Judiciário (CSCPJ). DJe/CNJ nº 361/2020, p. 5-6, 16 nov. 2020.

_____. **Resolução nº 361, de 17 de dezembro de 2020**. Determina a adoção de Protocolo de Prevenção a Incidentes Cibernéticos no âmbito do Poder Judiciário (PPICiber/PJ). DJe/CNJ nº 397/2020, p. 4-6, 17 dez. 2020.

_____. **Ato Normativo**. Processo nº 0010158-46.2020.2.00.0000, Rel. Cons. Luiz Fux. 323ª Sessão Ordinária, julgado em 15/12/2020.

GARGARELLA, Roberto. Constitutionalism of the Global South. **International Journal of Constitutional Law**, v. 15, issue 2, p. 571-573, April 2007.

HOFFMANN-RIEM, Wolfgang. **Teoria Geral do Direito Digital**: transformação digital e desafios para o direito. Rio de Janeiro: Forense, 2021.

MENDES, Laura Schertel. Proteção de dados pessoais: fundamento, conceitos e modelo de aplicação. **Panorama setorial da Internet**, ano 11, n. 2, p. 1-7, jun. 2019.

_____; MATTIUZO, Marcela. Discriminação Algorítmica: conceito, fundamento legal e tipologia. **Revista de Direito Público**, Porto Alegre, v. 16, n. 90, pp. 39-64, nov./dez. 2019.

_____; FONSECA, Gabriel Campos Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **Revista Estudos Institucionais**, Rio de Janeiro, v. 6, n. 2, p. 507-533, maio/ago. 2020.

_____; _____. STF reconhece direito fundamental à proteção de dados: comentários sobre o referendo da Medida Cautelar nas ADIs 687, 6388, 6389, 6390 e 6393. **Revista de Direito do Consumidor**, vol. 130/2020, p. 471-478, jul./ago. 2020.

MENKE, Fabiano. A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. **Revista Jurídica Luso-Brasileira**, ano 5, n. 1, p. 781-809, 2019.

SADEK, Maria Tereza (org.). **O Sistema de Justiça**. Rio de Janeiro: Centro Edelstein de Pesquisas Sociais, 2010.

SILVEIRA, Sérgio Amadeu. Ciberativismo, cultura hacker e o individualismo colaborativo. **Revista USP**, v. 1, p. 28-39, 2010.

SIMITIS, Spiros. Reviewing privacy in an information society. **University of Pennsylvania Law Review**, v. 135, p. 707-746, 1987.

SUPREMO TRIBUNAL FEDERAL (STF). **Resolução nº 612, de 23 de abril de 2018**. Dispõe sobre a Política Corporativa de Segurança da Informação (PCSI/STF). DJE/STF nº 80/2018, p. 3-5, 25 abr. 2018.

_____. **Resolução nº 724, de 02 de março de 2021**. Institui o Comitê Executivo de Proteção de Dados para identificar e implementar as medidas necessárias à adequação do Supremo Tribunal Federal às exigências da Lei n. 13.709, de 14 de agosto de 2019 (Lei Geral de Proteção de Dados - LGPD). DJE/STF nº 40, p. 1, 04 mar. 2021.

VAN DIJCK, Johana. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. **Surveillance & Society**, v. 12, n. 2, p. 197-208, 2014.