REVISTA DA

ESCOLA NACIONAL DA MAGISTRATURA

A JUSTIÇA DO TRABALHO NO MUNDO PÓS-PANDÊMICO

Organização Científica

Renata Gil de Alcantara Videira

Caetano Levi Lopes

Claudia Marcia Carvalho Soares

Paulo Roberto Dornelles Junior

ENM
ESCOLA NACIONAL DA MAGISTRATURA

Nº 11

A LEI GERAL DE PROTEÇÃO DE DADOS E O PROCESSO DO TRABALHO NO CONTEXTO DA "JUSTIÇA 4.0"

Ministro Aloysio Corrêa da Veiga[173]
Roberta Ferme Sivolella[174]

Resumo: O presente artigo pretende abordar os aspectos mais relevantes do sistema de proteção de dados no Brasil, a partir do advento da Lei n. 13.709/2021. Por meio da análise da evolução do tratamento legal acerca do tema nos Estados Unidos e na Europa, busca-se identificar os princípios e os fundamentos que irão nortear os debates acerca do direito à proteção de dados no âmbito do processo judicial eletrônico e, em especial, no processo do trabalho. Considerando-se que o contexto da pandemia e da virtualização dos atos processuais acelerou a incorporação das novas ferramentas tecnológicas no cotidiano da prática judicial, examina-se a compatibilização entre o direito fundamental do titular dos dados, o interesse público envolvido, e a finalidade do processo, sob o enfoque do tratamento normativo dado à matéria pelo Conselho Nacional de Justiça, e as peculiaridades do processo do trabalho frente à "Justiça 4.0".
Palavras-chave: Lei Geral de Proteção de Dados; Processo Judicial Eletrônico; processo do trabalho; direitos fundamentais; interesse público.

INTRODUÇÃO

Ao longo de sua origem e evolução, o Direito ocupa-se com a observação e as respostas às necessidades sociais de seu tempo. O processo, como materialização de tais expectativas, acompanhou a preocupação com a efetividade dos direitos, trazendo a ruptura de uma visão restrita ou

[173] Corregedor-Geral da Justiça do Trabalho.
[174] Juíza Auxiliar da CGJT.

individualista do processo, passou a apresentar uma característica de coletivização ou socialização da estrutura processual.[175]

Em meio às novas ferramentas tecnológicas para a prática de atos processuais, a incorporação de práticas automatizadas advindas da denominada Revolução 4.0 no mundo dos fatos e do direito, e a circulação cada vez mais rápida de dados e informações, a urgência decorrente da grande crise social e sanitária advinda da pandemia do Covid-19 trouxe ao Poder Judiciário novos dilemas e inquietações.

A psicanálise, há tempos, já prenuncia que a criatividade advém tanto dos contextos de crise, quanto dos de abundância.[176] Os extremos, por sua vez, costumam chamar a atenção da humanidade para questões que necessitam de aprofundamento e proteção, principalmente em se tratando de direitos fundamentais, seara de atuação constante e atenta do processo do trabalho.

No caso da temática da proteção de dados, os dilemas trazidos por sua aplicação no contexto de atos virtuais realizados e do Processo Judicial Eletrônico demandam atenção e aprofundamento, na medida em que envolvem direitos fundamentais sob todos os seus aspectos.

O direito alemão, em conceitos invocados pelo STF, preleciona que os direitos fundamentais não podem ser considerados apenas proibições de intervenção (*Eingriffsverbote*), mas expressam também um postulado de proteção (*Schutzgebote*); expressam não apenas uma proibição do excesso (*Übermassverbote*), como também podem ser traduzidos como proibições de proteção insuficiente ou imperativos de tutela (*Untermassverbote*).[177]

Nesse contexto, a vigência da Lei n. 13.709/2018 (LGPD) iniciada em setembro de 2020 enseja grandes debates sobre a sua aplicação e interpretação no cotidiano do processo do trabalho, em meio ao contexto de crise citado e às novas ferramentas processuais incorporadas ao cotidiano das audiências

---

[175] SIVOLELLA, Roberta Ferme. A aplicação supletiva e subsidiária do novo CPC – distinções:...por uma visão dialógica da subsidiariedade e supletividade do Novo CPC frente à CLT: processualismo e argumentação. *In: BELMONTE, Alexandre Agra; DUARTE NETO, Bento Herculano; FREIRE e SILVA, Bruno* (coord.). ***O novo CPC aplicado ao processo do trabalho***. São Paulo: LTr, 2016. p. 117.

[176] WINNICOTT, Donald. Freedom. **Nouv. Rev. Psychanal**., 1986, p. 228-238.

[177] A menção aos conceitos citados consta da ementa do acórdão proferido nos autos do HC 102.087/MG, de relatoria do Ministro Celso de Mello, redator Ministro Gilmar Mendes, Segunda Turma, DJe 14.08.21.

trabalhistas. Nos próximos tópicos, o presente artigo pretende abordar, de maneira sucinta, as origens do direito à proteção de dados e seu tratamento ao redor do mundo, a fim de possibilitar a compreensão do contexto da edição da Lei de Proteção Geral de Dados no Brasil, e sua aplicação no processo do trabalho em face das novas ferramentas tecnológicas utilizadas.

1. ORIGENS HISTÓRICAS E CONTEXTO MUNDIAL DO DIREITO À PROTEÇÃO DE DADOS

Principalmente desde o pós-grandes guerras datado do século XX, o grande afluxo de informações e os primeiros inventos telemáticos alavancaram o que se denominou de "movimento de globalização". Com a criação dos grandes blocos econômicos, nas décadas de 70 e 80 do século passado, o aumento de circulação transfronteiriça de dados e informações em processos automatizados chamaram a atenção da sociedade mundial para a necessidade de sua regulamentação e limitação.

Alguns anos mais tarde, a denominada "Revolução 4.0" demonstrou avanço para a esfera jurisdicional, fazendo que conceitos como *big data*, *analytics, machine learning*[178] e computação cognitiva se imiscuam em conceitos jurídicos que já levaram alguns autores a identificar a existência de um fenômeno decorrente da aplicação da inteligência artificial ao Direito: a chamada **Jurisdição 4.0**,[179] ou, nos eixos regulamentados posteriormente pelo Conselho Nacional de Justiça, a "**Justiça 4.0**".

[178] Acerca dos conceitos, *vide*: LANEY, Doug B. **Infonomics***:* how to monetize, manage, and measure information as an asset for competitive advantage. *Routledge: Abingdon, 2017; HILBERT, Martin; LOPEZ, Priscila. The world's technological capacity to store, communicate, and compute information.* ***Science****, v. 332, n. 6025, p. 60-65, 2011. Disponível em:* www.sciencemag.org. Acesso em: 18 ago. 2021.

[179] O termo começa a ser utilizado em artigos nacionais sobre o tema, como em: FERREIRA, Rafael Fonseca. Jurisdição 4.0 e inteligência artificial exegética: os novos "códigos". **Conjur**. 2019. Disponível em: https://www.conjur.com.br/2019-abr-20/diario-classe-jurisdicao-40-inteligencia-artificial-exegetica-novos-codigos. Acesso em: 25 ago. 2021.

Em 2019, no contexto pré-pandêmico, o Grupo de Especialistas de Alto Nível em Inteligência Artificial da Comissão Europeia[180] já havia detectado algumas das preocupações iniciais advindas de um sistema de inteligência artificial que se espraia e atravessa as fronteiras globais. A necessidade de guarnecimento de uma sociedade equitativa e de proteção dos direitos fundamentais; a confiabilidade, robustez e segurança dos dados; a transparência e rastreabilidade; a prevenção contra a discriminação, respeito à diversidade e acessibilidade; o bem-estar social e ambiental; e a prestação de contas, são alguns dos pilares que sustentam o sistema atual de dados e que remonta, em suas origens jurídicas, ao período de reconhecimento dos direitos fundamentais pelo direito transnacional.

Seja na Declaração Universal de Direitos Humanos de 1948, em seu artigo 12 ("Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei"); na Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, de 1950, em seu artigo 8º ("Direito ao respeito pela vida privada e familiar 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros"), ou no Pacto de San José da Costa Rica, de 1969, em seu artigo 11 ("Proteção da Honra e da Dignidade 1. Toda pessoa tem direito ao respeito de sua honra e ao reconhecimento de sua dignidade. 2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação. 3. Toda pessoa tem direito à proteção da lei contra

[180] **Inteligência artificial**: a Comissão avançou com os seus trabalhos sobre as orientações deontológicas. E. Europa. eu. 2019. Disponível em: https://ec.europa.eu/commission/presscorner/detail/pt/IP_19_1893. Acesso em: 10 out. 2019.

tais ingerências ou tais ofensas"), é possível se perceber a preocupação da privacidade, da honra, da intimidade e, como supedâneo maior, da dignidade como arcabouços da preocupação com a exposição e o compartilhamento de dados pessoais.

Os modelos protetivos dos Estados Unidos e da Europa são bem ilustrativos das formas de abordagem adotadas e serviram de inspiração ao modelo de proteção adotado no Brasil.

1.1 O modelo protetivo americano

Nos Estados Unidos, o reconhecimento do *right of privacy* é indicado pela doutrina sobre o tema como o marco caracterizados do modelo de proteção de dados adotado no país.[181] A expressão concernente ao direito à privacidade (*The right of privacy*), inobstante disseminada no artigo de Samuel Warren e Louis Brandeis datado de 1890,[182] percorreu caminho de nuanças próprias na doutrina e na jurisprudência do país.

Inicialmente identificada como decorrência do direito à vida previsto na Quinta Emenda à Constituição Americana e na Declaração de Independência dos Estados Unidos, o direito à privacidade acabou sendo visto sob dois aspectos, conforme a existência ou não de exploração da imagem anterior à suposta lesão por seu titular, seja pessoa pública (*publicity*) ou particular (*privacy*).[183]

Os precedentes estado-unidenses sobre a matéria foram impulsionados pela exploração da imagem e o direito à proteção do titular sobre tal viés, a partir da invenção e da disseminação do uso da fotografia, como primeiro

---

[181] Sobre a questão, *vide*: SILVA, Thiago Rodrigo G. A privacidade, a proteção de dados e o direito de família. **Legale Scientia,** UNIMES, ed. especial, p. 94-99, 2021. Disponível em: https://periodicos.unimesvirtual.com.br/index.php/direito. Acesso em: 29 ago. 2021.

[182] "***The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world****, and man, under the refining influence of culture, has become more sensitive to publicity,* ***so that solitude and privacy have become more essential to the individual****; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury*" (WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard Law Review**, v. 4, n. 5, p. 193-220, dez. 1890, p. 196).

[183] ROTHMAN, Jennifer. The right of publicity: privacy reimagined for a public world. Boston: Harvard University Press, 2018.

veículo de circulação de dados utilizado. Os danos, nesses casos, eram considerados como danos *in re ipsa*, independendo de prova desde que versassem sobre hipóteses de exploração da imagem, de maneira não consentida, e com intuito comercial, denotando o caráter de proteção voltada ao direito do consumidor que iria permear o restando do caminho jurisprudencial percorrido. Como exemplos, podem ser citados os casos Roberson vs. Rochester Folding Box Co (caso *Flour for the family*, de 1902),[184] no qual o direito à imagem foi analisado junto ao direito de imprensa e a liberdade de expressão; Pavesich vs. New England Life Ins. Co. (em decisão da Suprema Corte da Geórgia, em 1905),[185] com o reconhecimento de responsabilidade civil decorrente do uso da imagem não consentido e com uso comercial, em violação à liberdade e à autodeterminação, e Olmstead vs. United States (1928), em que a direito à proteção à privacidade foi analisada, em relação aos dados interceptados telefonicamente pelo FBI, como decorrência do direito de propriedade. Considerou-se, no caso, que não teria havido a invasão física na propriedade, uma vez que os cabos telefônicos estavam em via pública.[186]

Contudo, somente em 1965, com o julgamento do caso Griswold vs. Connecticut, houve a indicação, pela doutrina, do reconhecimento constitucional pela Suprema Corte americana acerca do *right of privacy*, a partir da interpretação das seguintes emendas à Constituição dos Estados Unidos: primeira (liberdade de expressão), terceira (inviolabilidade do domicílio), quarta (vedação à busca e apreensões ilícitas), quinta (proteção contra a autoincriminação) e nona (ainda que não expressamente indicados,

---

[184] KORNSTEIN, Daniel J. The Roberson Privacy Controversy. **The Historical Society of the Courts of the State of New York**, Issue 4, 2006. Disponível em: https://www.nycourts.gov/history/programs-events/images/Judicial-Notice-Newsletter-04.pdf. Acesso em: 4 ago. 2021.

[185] ALLEN, Anita L. *Natural Law, Slavery, and the Right to Privacy Tort.* **Fordham L. Review**, v. 81, Issue 3, 2013. Disponível em: https://ir.lawnet.fordham.edu/flr/vol81/iss3/8. Acesso em: 5 ago. 2021.

[186] United States Supreme Court. 277 US 438 (1928) **Olmstead *et al.* vs. United States. Green *et al.* v. Same. McInnis vs. Same**. Argued Feb. 20 and 21, 1928. Decided June 4, 1928. Disponível em: https://www.law.cornell.edu/supremecourt/text/277/438. Acesso em: 10 ago. 2021.

os direitos fundamentais que dão corpo à Declaração de Direito são também protegidos por ela).[187]

A decisão da Suprema Corte de 1965 foi crucial para deslocar a proteção de dados do prisma único da propriedade, ampliando-o para os diversos enfoques envolvendo direitos fundamentais previstos explícita ou implicitamente na Constituição americana. Apesar de seguirem primordialmente sob o prisma do direito consumerista, a proteção de dados no direito americano seguiu tal interpretação não restritiva, como pôde se verificar em julgamentos mais recentes.

Nesse ponto, é relevante citar o caso Rosenbach vs. Six Flags**,** julgado em janeiro de 2019, em interpretação à Lei de Privacidade de Informações Biométricas de Illinois ("BIPA"– Illinois Biometric Information Privacy Act). No referido julgado, a Suprema Corte de Illinois, por unanimidade, reverteu a decisão do tribunal de apelação do estado, que havia considerado que a mera violação técnica da lei, sem a demonstração do dano pessoal gerado, seria insuficiente para conferir legitimidade ao titular dos dados para mover a ação como pessoa "prejudicada". Em interpretação sistemática da constituição e dos artigos 15 (b) e 29 da lei de privacidade de dados biométricos,[188] entendeu-se que o prejuízo advém da própria violação legal,

---

[187] GRISWOLD, Estelle T. *et al*. **Appellants, vs. State of Connecticut. n. 496**. Argued March 29, 1965. Decided June 7, 1965. Disponível em: https://www.law.cornell.edu/supremecourt/text/381/479. Acesso em: 20 ago 2021.

[188] Em tradução livre do original: *Section* 15 (b): a entidade privada que coletar ou usar as informações biométricas de uma pessoa deve (1) informar a pessoa por escrito que suas informações biométricas estão sendo coletadas, (2) explicar a finalidade e o período de tempo durante o qual as informações serão ser usado e (3) receber consentimento por escrito. Section 20 – direito privado de ação por parte de qualquer "prejudicado" por violação a esta lei, para ressarcimento de danos. A mesma lei traz esmiuçados conceitos a respeito da coleta e transmissão de dados biométricos protegidos pelos artigos que a compõem, em seu artigo 10, *verbis*:

"Sec. 10. Definitions. In this Act":"Biometric information" *means any information, regardless of how it is captured, converted, stored, or shared, based on an* ***individual's biometric identifier used to identify an individual****. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.****"Confidential and sensitive information"*** *means personal information that can be used to uniquely identify an individual or an individual's account or property.* ***Examples of confidential and sensitive information include, but are not limited to, a genetic marker, genetic testing information, a unique identifier number to locate an account or property, an account number, a PIN number, a pass code, a driver's license number, or a social security number."Private entity"*** *means any individual, partnership, corporation, limited*

a partir do momento em que os titulares dos dados não são informados acerca do destino dos dados coletados, tampouco manifestaram sua autorização expressa na coleta e no compartilhamento.[189]

Os EUA não possuem uma lei de proteção de dados de abrangência nacional. Há várias leis versando sobre a privacidade do cidadão em relação a seus dados, além acordos de proteção de dados assinados com a União Europeia e a Suíça. Em 2018, a Califórnia editou a lei de proteção de dados relativamente ao cadastro de consumidores California Consumer Privacy Act (CCPA or Act), vigente a partir de 1º de janeiro de 2020. Nos primeiros 7 meses de vigência da lei, cerca de 50 ações foram movidas sob a alegação de pretensa violação às regras trazida, seja sob a ótica do direito do consumidor, seja sob a ótica da violação de dados, em números expressivos no comparativo do cotidiano de judicialização do país. A maioria de tais ações foi interposta por meio de *class actions,* o que revela o caráter de interesse público que envolve a matéria e que também se mostra presente no tratamento dado à questão no Brasil. A maioria dos casos foi resolvida por meio de arbitragem.[190]

Os Estados Unidos seguem sem uma lei geral de proteção de dados, possuindo jurisprudência e leis locais voltadas à tal interpretação ampla, que abarca visão inspirada primordialmente no sistema europeu de proteção de dados, como se verá.

---

liability company, association, or other group, however organized. A private entity does not include a State or local government agency. ***A private entity does not include any court of Illinois, a clerk of the court, or a judge or justice thereof."Written release"*** *means informed* ***written consent or, in the context of employment, a release executed by an employee as a condition of employment.*****"** (Source: P.A. 95-994, eff. 10-3-08.). Disponível em: https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57. Acesso em: 2 set. 2021.

[189] KIM, Tae. Rosenbach v. Six Flags: Illinois Supreme Court Interprets Illinois Biometric Privacy Law. *In*: **Harvard Journal of Law & Technology – Jolt Digest**. Boston, 2019. Disponível em: https://jolt.law.harvard.edu/digest/rosenbach-v-six-flags-illinois-supreme-court-interprets-illinois-biometric-privacy-law. Acesso em: 3 set. 2021.

[190] Um dos exemplos indicativos de ação movida por conta de compartilhamento de dados em redes sociais é a **Class Action Complaint and Demand for Jury Trial**, G.R. v. TikTok, Inc., n. 2:20-cv-04537 (C.D. Cal. May 20, 2020), ECF No. 1. Disponível em: https://www.classaction.org/media/slate-et-al-v-tiktok-inc-et-al.pdf. Acesso em: 10 set. 2021.

1.2 O modelo protetivo europeu

O modelo europeu de proteção de dados apresenta características, em sua origem e evolução, que inspiraram os princípios constantes da Lei n. 13.709/2018. Como marco dessa evolução, o Tribunal Constitucional Alemão reconheceu, em 1983, o direito fundamental à autodeterminação informativa, como direcionador de uma tutela autônoma da proteção de dados, garantindo ao cidadão a palavra final no controle de seus dados, e que não se confunde com a tutela geral à privacidade.[191]

Em 2000, a Carta de Direitos Fundamentais da União Europeia repetiu tal entendimento, ao indicar, em seu artigo 8º, o reconhecimento da Proteção de Dados como um direito autônomo, destacado do Direito à Privacidade previsto em seu artigo 7º.[192] Cinco anos antes, a Diretiva Europeia número 95/46/CE trazia importante contribuição acerca do caráter fundamental e de interesse público que envolve o direito à proteção de dados, ao prever, em seu artigo 2º, que "os sistemas de tratamento de dados estão ao serviço do Homem; que devem respeitar as liberdades e os direitos fundamentais das pessoas singulares independentemente da sua nacionalidade ou da sua residência, especialmente a vida privada, e contribuir para o progresso económico e social, o desenvolvimento do comércio e o bem-estar dos indivíduos".[193]

A Resolução n. 679/2016, denominada "General Data Protection Regulation (GDPR)" passou a expressamente exigir, a partir de sua vigência, em 25 de maio de 2018, a informação aos titulares dos dados sobre eventuais incidentes envolvendo o compartilhamento de informações; sobre a prova do consentimento, portabilidade de dados, indicação e responsabilidade dos agentes encarregados pela operacionalidade dos dados; e sobre as regras de segurança para armazenamento, transmissão e manuseio. Apresentou, ainda,

---

[191] MENKE, Fabiano. A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: **RJLB**, ano 5, n. 1, p. 781-809, 2019. Disponível em: http://www.cidp.pt/revistas/rjlb/2019/1/2019_01_0781_0809.pdf. Acesso em: 10 set. 2021.

[192] Cf. U.E. Carta dos Direitos Fundamentais da União Europeia. *In*: **Jornal Oficial das Comunidades Europeias C 364/1**, 18 dez. 2000. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 2 ago. 2021.

[193] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 2 ago. 2021.

detalhada conceituação de “dados biométricos”, “dados de saúde” e “dados genéticos”, conjuntamente com os “dados sensíveis”.[194]

Com efeito, assim dispõe o seu artigo 2º:

> “Artigo 2º
> Âmbito de aplicação material
> 1. O presente regulamento aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados.
> 2. O presente regulamento não se aplica ao tratamento de dados pessoais:
> a) Efetuado no exercício de atividades não sujeitas à aplicação do direito da União;
> b) Efetuado pelos Estados-Membros no exercício de atividades abrangidas pelo âmbito de aplicação do título V, capítulo 2, do TUE;
> c) Efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas;
> d) Efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública.
> 3. O Regulamento (CE) n. 45/2001 aplica-se ao tratamento de dados pessoais pelas instituições, órgãos, organismos ou agências da União. O Regulamento (CE) n. 45/2001, bem como outros atos jurídicos da União aplicáveis ao tratamento de dados pessoais, são adaptados aos princípios e regras do presente regulamento nos termos previstos no artigo 98º.
> 4. O presente regulamento não prejudica a aplicação da Diretiva 2000/31/CE, nomeadamente as normas em

[194] Cf. U.E. Carta dos Direitos Fundamentais da União Europeia (2016/C 202/02). In: **Jornal Oficial da União Europeia C 202/389**. 7 jun. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR. Acesso em: 2 ago. 2021.

> matéria de responsabilidade dos prestadores intermediários de serviços previstas nos seus artigos 12º. a15º.[195]

Como se verifica do referido artigo transcrito, o Regulamento n. 45/2001 regulamenta particularmente o tratamento de dados pessoais por parte de órgãos governamentais. Em sua seção 2, artigo 5º, apresenta princípios que se compatibilizam com aqueles previstos no ordenamento brasileiro, a saber:

> Regulamento (CE) n. 45/2001
> SECÇÃO 2
> PRINCÍPIOS RELATIVOS À LEGITIMIDADE DO TRATAMENTO DE DADOS
> Artigo 5º Licitude do tratamento
> O tratamento de dados pessoais **só pode ser efectuado se**:
> a) For necessário ao exercício de **funções de interesse público** com fundamento nos Tratados que instituem as Comunidades Europeias ou noutros actos legislativos aprovados com base nesses Tratados, ou no **exercício da autoridade pública de que estão investidos a instituição ou o órgão comunitário ou um terceiro a quem os dados sejam comunicados**; ou
> b) **For necessário para o respeito de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito**; ou
> c) For necessário para a execução de um contrato no qual a pessoa em causa é parte ou de diligências pré-contratuais a pedido da pessoa em causa; ou
> d) **A pessoa em causa tiver dado de forma inequívoca o seu consentimento**; ou
> e) **For necessário para a protecção de interesses vitais da pessoa em causa**.[196]

[195] *Idem*.
[196] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32001R0045. Acesso em: 2 ago. 2021.

A análise sistemática da Resolução CE n. 679/2016 e da Resolução CE 45/2001 permite concluir pela incorporação das seguintes características ao modelo europeu de proteção de dados: (*i*) reconhecimento do direito à proteção de dados, sob o viés duplo do i.1) tratamento e do i.2) compartilhamento/transmissão, como direito fundamental e autônomo; (*ii*) reconhecimento da presença do interesse público como norteador dos limites e exceções ao tratamento e transmissão e dados; (*iii*) reconhecimento da autodeterminação informativa (também sob duplo viés, a saber iii.1) necessidade de consentimento do titular em relação ao fornecimento, tratamento e transmissão de dados, e iii.2) necessidade de ampla informação do titular acerca das características de tais atos) como princípio geral do sistema de proteção de dados. Tais características foram o mote da criação dos modelos legais de proteção de dados de outras nações, a exemplo do Brasil.

2. LEI GERAL DE PROTEÇÃO DE DADOS NO BRASIL

A Lei Geral de Proteção de Dados (LGPD), aprovada em 2018 sob o número 13.709 no Brasil e objeto de intenso debate, teve o início de sua vigência postergado em virtude da pandemia do Covid-19 para 18 de setembro de 2020, muito embora as tentativas de postergação a *vacatio legis* apontassem para maio de 2021.

Por certo, o amplo espectro de sua aplicação, apontado já pela previsão textual de seus primeiros artigos, contribuiu para a preocupação acerca das dúvidas que poderiam advir sobre sua abrangência, e da necessidade de adaptação das incontáveis e cada vez mais incorporadas em nosso cotidiano ferramentas tecnológicas, hábeis e minuciosos instrumentos de dados por sua própria natureza.

Com efeito, nos termos do artigo 3º da LGPD, se inserem no âmbito de aplicação da lei "qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país no qual estejam localizados os dados", desde que (*i*) a operação de tratamento de dados seja realizada no Brasil; (*ii*) a atividade de tratamento tenha por objetivo a oferta

de bens ou serviços ou o manejo de dados de indivíduos localizados no país; ou, ainda, (*iii*) que os dados pessoais objeto do tratamento tenham sido coletados em território nacional. (Art. 3º)

Não se inserem no escopo da lei, nos termos do artigo 4º, o tratamento de dados pessoais realizado por pessoa natural para fins exclusivamente particulares e não econômicos (inciso I); realizado para fins exclusivamente jornalísticos, artísticos (inciso II, a), acadêmicos (inciso II, b), além de informações relacionadas exclusivamente à segurança pública (inciso III, a), defesa nacional (inciso III, b), segurança do Estado (inciso III, c) e a atividades de investigação e repressão de infrações penais (inciso III, d). Nas hipóteses do inciso III, o parágrafo 1º, do artigo 4º, expressamente prevê que tais informações estarão submetidas à regência de legislação específica, que deverá prever "medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular" previstos na mesma lei.

A existência da palavra "ou" no artigo 3º, no sentido de tornar alternativa, e não condicionante, a circunstância do tratamento de dados se referir à oferta de bens e serviços para que esteja sob a alçada da Lei n. 13.709/2018, torna ainda mais consistente a interpretação da amplitude do alcance da lei, aplicável a todo o tratamento de dados realizado no território nacional, com exceção das hipóteses expressamente previstas no artigo 4º.

Por sua vez, a indicação da palavra "e" no inciso I do referido artigo 4º, ao indicar como necessária à concomitância do uso dos dados para fins exclusivamente particulares, e não econômicos, repisa a constatação de que o critério de oferta de bens e a finalidade econômica do tratamento de dados não seriam requisitos indispensáveis para identificar a aplicação da lei, quando o referido tratamento é atinente a órgãos e finalidades públicas. Nesse sentido, o mesmo artigo acaba por tornar claras as hipóteses que expressamente não são abarcadas pela lei, entre as quais, intimamente ligadas com o interesse público e o tratamento de dados realizado por órgãos públicos, estão a segurança pública e de Estado, a defesa nacional, e as atividades de investigação e repressão a infrações penais. Essa última exceção tem trazido debates acerca da inclusão da atividade de tratamento de dados em relação a processos judiciais, independentemente de se circunscreverem a matérias penais.

Independentemente da interpretação que se dê, o fato é que o parágrafo 1º do artigo 4º aqui repisado demonstra toda a cautela e as restrições trazidas pela legislação, mesmo nas hipóteses excetuadas citadas, devendo observar medidas proporcionais e estritamente necessárias ao atendimento do interesse público, e sempre em observância ao devido processo legal, aos princípios gerais de proteção e aos direitos do titular. Sob tal prisma, a lei procurou trazer a obrigatoriedade da observância, em qualquer hipótese, dos princípios afetos à proteção de dados e a obrigatoriedade do interesse público como finalidade a ser perseguida sempre, como justificativa a respaldar o permissivo ao manejo dos dados do titular.

Assemelhando-se às características trazidas pelo modelo europeu, o modelo brasileiro de proteção de dados trazido pela LGPD também tratou do direito do titular como direito fundamental, e sujeito à autodeterminação informativa, tal e qual claramente se verifica nos fundamentos trazidos pelo artigo 2º da Lei 13.709/18.[197]

Os princípios gerais dispostos no artigo 6º, por sua vez, amoldam-se com os conceitos de adstrição à finalidade, e sua adequação com o tratamento destinado aos dados e à sua necessidade, correspondente à limitação do permissivo ao tratamento de dados "ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados"; cuja transparência, livre acesso e a segurança das informações devem estar acessíveis ao titular a qualquer tempo.[198] De tais princípios de observância

[197] Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: I – o respeito à **privacidade**; II – a **autodeterminação informativa**; III – a liberdade de expressão, de informação, de comunicação e de opinião; IV – a **inviolabilidade da intimidade, da honra e da imagem**; V – o desenvolvimento econômico e tecnológico e a inovação; VI – a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII – os direitos humanos, o livre desenvolvimento da personalidade, **a dignidade** e o exercício da cidadania pelas pessoas naturais.

[198] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I – **finalidade**: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II – **adequação**: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; **III – necessidade:** limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; **IV – livre acesso**: garantia, aos titulares, de

obrigatória emerge a reponsabilidade daquele que realiza o referido tratamento, assim considerado, nos termos do inciso X do artigo 5º, "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração". Os agentes de tratamento são, respectivamente, o controlador ("pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" – artigo 5º, VI), e o operador ("operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador"– artigo 5º, VII). Observa-se, assim, que passam a ser responsáveis, nos termos da lei, todos aqueles que tomam decisões concernentes ao acesso, utilização, avaliação dos dados, armazenamento e difusão das informações armazenadas.

Os dados pessoais protegidos, por sua vez, também não encontram restrição de conceito, referindo-se, nos termos do artigo 5º, I da LGPD, a toda e qualquer informação relacionada à pessoa natural identificada ou identificável, sendo considerados sensíveis todos os dados pessoais relacionados à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (art. 5º, inciso II, da LGPD).

---

consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; **V – qualidade dos dados:** garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; **VI – transparência:** garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; **VII – segurança:** 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; **VIII – prevenção**: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; **IX – não discriminação:** impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; **X – responsabilização e prestação de contas**: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

É interessante observar que, mesmo antes da entrada em vigor da Lei 13.709/2018, o STF já utilizava o tratamento da proteção de dados como atinente a direito fundamental do titular, sujeito à autodeterminação informativa, ao interesse público envolvido e aos limites determinados pelo tratamento adequado, relevante e não excessivo em relação a sua finalidade.[199] Tal entendimento traz a lume não só com os expressamente

[199] MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE. REFERENDO. MEDIDA PROVISÓRIA N. 954/2020. EMERGÊNCIA DE SAÚDE PÚBLICA DE IMPORTÂNCIA INTERNACIONAL DECORRENTE DO NOVO CORONAVÍRUS (COVID-19). **COMPARTILHAMENTO DE DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO FIXO COMUTADO E DO SERVIÇO MÓVEL PESSOAL, PELAS EMPRESAS PRESTADORAS, COM O INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA.** FUMUS BONI JURIS. PERICULUM IN MORA. DEFERIMENTO.
1. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais. 2. Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, *caput*), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados. 3. O Regulamento Sanitário Internacional (RSI 2005) adotado no âmbito da Organização Mundial de Saúde exige, quando essencial o tratamento de dados pessoais para a avaliação e o manejo de um risco para a saúde pública, a garantia de que os dados pessoais manipulados sejam **"adequados, relevantes e não excessivos em relação a esse propósito" e "conservados apenas pelo tempo necessário."** (artigo 45, § 2º, alíneas "b" e "d"). 4. Consideradas a **necessidade, a adequação e a proporcionalidade da medida,** não emerge da Medida Provisória n. 954/2020, nos moldes em que editada**, interesse público legítimo** no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia. 5. Ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP n. 954/2020 desatende a garantia do devido processo legal (art. 5º, LIV, da CF), na dimensão substantiva, por 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. 6. **Ao não apresentar mecanismo técnico ou administrativo apto a proteger**, de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão, seja no tratamento, o sigilo, a higidez e, quando o caso, o anonimato dos dados pessoais compartilhados, a MP n. 954/2020 descumpre as exigências que exsurgem do texto constitucional no tocante à efetiva proteção dos direitos fundamentais dos brasileiros. 7. Mostra-se **excessiva** a conservação de dados pessoais coletados, pelo ente público, por trinta dias após a decretação do fim da situação de emergência de saúde pública, tempo manifestamente excedente ao estritamente necessário para o atendimento da sua finalidade declarada. 8. Agrava a **ausência de garantias de tratamento adequado e seguro dos dados** compartilhados a circunstância de

citados incisos X e XII, e *caput*, do artigo 5º da Constituição Federal, mas também com as disposições contidas no inciso LX do mesmo artigo 5º constitucional ("a lei só poderá restringir a publicidade dos atos processuais quando a defesa da intimidade ou o interesse social o exigirem"), e do inciso IX do artigo 93 do mesmo diploma maior ("todos os julgamentos dos órgãos do Poder Judiciário serão públicos, e fundamentadas todas as decisões, sob pena de nulidade, podendo a lei limitar a presença, em determinados atos, às próprias partes e a seus advogados, ou somente a estes, em casos nos quais a preservação do direito à intimidade do interessado no sigilo não prejudique o interesse público à informação").

A preocupação do legislador constitucional com o interesse público e, ao mesmo tempo, com a preservação da privacidade do titular dos dados no processo judicial, traz à tona, mais uma vez, a discussão acerca do papel do Poder Judiciário e, em especial, do Juiz, em relação ao modelo de proteção de dados adotado pelo Brasil, em especial sob o enfoque de seu tratamento sob o prisma da natureza de direito fundamental do titular. Se, por um lado, é certo que a gestão de dados e informações no exercício da função jurisdicional não pode ser identificada de maneira simplória com o papel ordinário do controlador e o operador de dados, também é certo que a preocupação com a adequação e a necessidade do uso dos dados, que devem estar estritamente ligadas à finalidade do processo, precisa ser observada no manejo das novas ferramentas tecnológicas por todo o operador do direito. É recomendável que a determinação do fornecimento de dados sensíveis, desnecessários ao deslinde do processo e sem a observância dos princípios e requisitos previstos

---

que, embora aprovada, ainda não vigora a Lei Geral de Proteção de Dados Pessoais (Lei n.13.709/2018), definidora dos critérios para a responsabilização dos agentes por eventuais danos ocorridos em virtude do tratamento de dados pessoais. O fragilizado ambiente protetivo impõe cuidadoso escrutínio sobre medidas como a implementada na MP n. 954/2020. 9. O cenário de urgência decorrente da crise sanitária deflagrada pela pandemia global da Covid-19 e a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento **não podem ser invocadas como pretextos para justificar investidas visando ao enfraquecimento de direitos e atropelo de garantias fundamentais consagradas na Constituição**. 10. Fumus boni juris e periculum in mora demonstrados. Deferimento da medida cautelar para suspender a eficácia da Medida Provisória n. 954/2020, a fim de prevenir **danos irreparáveis à intimidade e ao sigilo da vida privada** de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel. **11. Medida cautelar referendada. STF: REFERENDO NA MEDIDA CAUTELAR NA ADIN 6.390/DF (07/05/2020, rel. Ministra Rosa Weber).**

para o seu tratamento sejam evitados, assim como a sua difusão e/ou o uso de meios de armazenamento que permitam o compartilhamento ilimitado desses dados.

Os artigos 7º e 11 da Lei n. 13.709/2021 trazem, nesse ponto, os requisitos necessários para que se considere legítimo o manejo de dados pessoais e dados pessoais sensíveis, respectivamente. Em ambos os casos, exprime-se a necessidade de expresso consentimento pelo titular, existência de obrigação legal pelo controlador, ou no exercício regular de direitos em processo judicial, em expressão que denota claramente a demanda de necessidade e utilidade específica ao fornecimento de tais dados, voltados à finalidade do processo.[200] É crucial, portanto, que o uso de ferramentas tecnológicas como meio de produção de atos processuais esteja atento a tais

[200] Assim dispõem os referidos artigos: "Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: **I – mediante o fornecimento de consentimento pelo titular; II – para o cumprimento de obrigação legal ou regulatória pelo controlador;** III – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; [...] VI – **para o exercício regular de direitos em processo judicial,** administrativo ou arbitral, esse último nos termos da Lei n. 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); VII – para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII – para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei n. 13.853, de 2019) IX – quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X – para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente"– g.n. **"Art. 11:** O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I – quando o titular ou seu responsável legal **consentir**, de forma específica e destacada, **para finalidades específicas;** II – **sem fornecimento de consentimento do titular**, nas hipóteses em que for indispensável para: a) **cumprimento de obrigação legal** ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) **exercício regular de direitos,** inclusive em contrato e **em processo judicial, administrativo** e arbitral, este último nos termos da Lei n. 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei n. 13.853, de 2019) g) **garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos,** resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais."

diretrizes, bem como à regulamentação específica que envolve o processo judicial, e as minúcias do cotidiano da realização de atos processuais trabalhistas.

3. A LGPD, O PROCESSO JUDICIAL ELETRÔNICO E O PROCESSO DO TRABALHO

Ao regulamentar o controle do sistema judicial pelo processo judicial eletrônico, o Conselho Nacional de Justiça, em 2013, já havia trazido previsão no sentido de que tal controle compreenderia não só a padronização de todos os dados e informações compreendidas pelo processo judicial, mas também a produção, o registro e a publicidade dos atos processuais, bem como a responsabilidade pelo fornecimento de dados essenciais à gestão das informações necessárias ao diversos órgãos de supervisão, controle e uso do sistema judiciário.[201]

Em 20 de agosto de 2020, o mesmo Conselho elegeu três pilares centrais a envolver a proteção de dados no tratamento das informações inseridas no fluxo do processo judicial eletrônico, e em meio ao panorama trazido pela Justiça 4.0 e seus instrumentos. Em seu artigo 1º, a Recomendação CNJ n. 73/2020 traçou um norte à elaboração de plano de ação pelos Tribunais (inciso I), envolvendo a indicação e a transparência em relação à organização e comunicação; aos direitos do titular; gestão de consentimento; retenção de dados e cópia de segurança; contratos; e plano de respostas a incidentes de segurança com dados pessoais; à disponibilização de informações ao titular nos sítios eletrônicos dos Tribunais (inciso II), atinente às informações básicas sobre a aplicação da Lei Geral de Proteção de Dados aos tribunais, incluindo os requisitos para o tratamento legítimo de dados, as obrigações dos controladores e os direitos dos titulares, bem como ao fornecimento de um formulário para exercício de direitos dos titulares de dados pessoais; e à elaboração ou adequação, com ostensiva publicação dos sítios eletrônicos, da política de privacidade da navegação, bem como o registro de dados pessoais (inciso III), envolvendo a finalidade do tratamento,

[201] Trata-se do artigo 2º da Resolução n. 185/2013 do Conselho Nacional de Justiça.

a base legal; a descrição dos titulares; a categorias de dados; a categorias de destinatários; a transferência internacional; o prazo de conservação; as medidas de segurança adotadas; e a política de segurança da informação.

Ao estabelecer tais diretrizes, o Conselho Nacional de Justiça acabou por estabelecer parâmetros a serem observados pelos Tribunais, em consonância aos fundamentos e princípios dispostos na LGPD, de modo a proteger e legitimar a atuação dos operadores e controladores de tais dados no processo judicial eletrônico, não só sob o prisma da atividade administrativa (originalmente direcionada pela lei de acesso à informação e pelo princípio da publicidade insculpido no artigo 37 da Constituição Federal), mas também em relação à atividade judicante. Em relação a esta, não há dúvida de que o intenso fluxo de dados e a nova dinâmica estabelecida pela denominada "Justiça 4.0", em todos os seus eixos, tornam cada vez mais difícil dissociar, por completo, o tratamento de dados no exercício da atividade puramente jurisdicional, daquele inserido na responsabilidade do controlador e operador de tais dados, já que tal tratamento também se refere, nos termos legais, a acesso, filtragem de dados, armazenamento, transmissão e compartilhamento de tais dados, acabando por abarcar, ainda que de maneira periférica, certo poder de escolha em relação a qual a sorte de dados que irá compor este aparato judicial de informações.

O aparato normativo que envolve a indicação de ferramentas de uso obrigatório para o tratamento de tais dados corrobora tal assertiva, podendo ser citadas, como exemplos, a Resolução CNJ n. 331, de 20 de agosto de 2020 (instituindo a Base Nacional de Dados do Poder Judiciário (DataJud) como fonte primária de dados do Sistema de Estatística do Poder Judiciário (SIESPJ) para os tribunais indicados nos incisos II a VII do art. 92 da Constituição Federal), a Resolução CNJ n. 335, de 29 de setembro de 2020 (instituindo a política pública para a governança e a gestão de processo judicial eletrônico, e integrando os tribunais do país com a criação da Plataforma Digital do Poder Judiciário Brasileiro – PDPJ-Br), a Resolução CNJ n. 345, de 9 de outubro de 2020 ("Juízo 100%¨digital"), a Resolução CNJ n. 354, de 19 de novembro de 2020 (dispondo sobre o cumprimento digital de ato processual e de ordem judicial); a Resolução CNJ n. 372, de 12 de fevereiro de 2021 (regulamentando a criação de plataforma de videoconferência denominada "Balcão Virtual") e a Resolução CNJ n. 385,

de 6 de abril de 2021 (criando os "Núcleos de Justiça 4.0" e dá outras providências).

No caso do processo do trabalho, algumas situações envolvendo atos processuais praticados por meio de tais ferramentas tendem a se tornar mais nebulosas, em relação à sistemática de proteção a ser aplicada no tocante aos dados lá fornecidos. Isso porque, no cotidiano da produção de tais atos processuais, torna-se muito comum o fornecimento de dados pessoais, não raro sensíveis, dada a alta carga fática que permeia as lides de natureza trabalhista.

Não há dúvida de que o formulário de consentimento e o plano de ação recomendado pelo Conselho Nacional de Justiça tornam inequívoco o permissivo do manejo de dados dentro da finalidade do processo, e de acordo com o livre convencimento motivado do Juiz. Contudo, como já dito, cautelas fazem-se recomendáveis envolvendo questões a que o cotidiano do Poder Judiciário ainda está incorporando, como é o caso da produção de provas digitais, e da videogravação de audiências, principalmente porque a proteção de dados envolve não só a expressa previsão dos dispositivos da LGPD, mas tira o seu supedâneo de direitos constitucionais fundamentais. Nesse sentido, a cooperação e a boa-fé, bem como os limites da liberdade de expressão e o manejo dos dados armazenados também posteriormente à prática do ato, devem ser observados.

A Resolução CNJ n. 105/2010 teve sua redação alterada em 2016 e 2020 por meio da Resoluções n. 222 e da n. 326, respectivamente, a partir do que o CNJ previu a disponibilização de sistemas eletrônicos de gravação dos depoimentos, dos interrogatórios e de inquirição de testemunhas por videoconferência, com possibilidade de desenvolvimento, também por parte dos Tribunais, de repositórios de mídias para armazenamento de documentos de som e imagem, inclusive os decorrentes da instrução do processo, e equivalência entre os documentos digitais inseridos no Repositório Nacional de Mídias para o Sistema PJe e as peças integrantes dos autos eletrônicos do processo judicial correspondente. O mesmo normativo previu, ainda, a dispensa da transcrição dos depoimentos obtidos pelos meios previstos na resolução em seu artigo 2º, determinando a preferência, no caso da testemunha arrolada não residir na sede do juízo em que tramita o processo, à expedição da carta precatória para a inquirição pelo sistema de

videoconferência, em observância ao princípio da identidade física do Juiz (artigo 3º da Resolução 105/2010). Tais determinações, com a redação alterada ao longo do tempo, trouxeram a preocupação com o uso específico e adequado dos dados ligados, estritamente, à finalidade do processo e ao interesse público, vedado o abuso inclusive em relação à divulgação posterior dissociada de tal finalidade, ou mesmo a exigência do fornecimento de informações sensíveis não adequadas, úteis e necessárias ao interesse público e ao escopo da atividade jurisdicional praticada. Tal proteção refere-se a todos os atores processuais, inclusive ao Juiz, relativamente ao uso e à divulgação de sua imagem e dados desconectados do escopo processual, ou descontextualizados em relação à prática de tais dados.

A proteção de dados sob o prisma da imagem, e do contexto em que praticados, em compatibilização ao princípio da publicidade, fica clara também na opção utilizada pelo Conselho Nacional de Justiça quando da edição da Resolução n. 354/20, quando, em seu artigo 7º, prevê, junto à obrigação do armazenamento de dados em repositório específico, a transmissão em tempo real do ato, de modo a possibilitar que terceiros estranhos ao feito, ainda que mediante autorização, acompanhem a sua prática. A previsão, portanto, é específica ao acompanhamento do ato processual, não permitindo o uso ou a divulgação abusiva ou descontextualizada dos dados que venham a ser submetidos a fluxo de compartilhamento quando da prática de tal ato.[202]

No caso da Justiça do Trabalho, a dinâmica de cartas precatórias também ganhou tratamento direcionado à prática do ato por meio telepresencial, sendo regulamentada pelo Provimento CGJT n. 1, de 16 de março de 2021. Na forma de seu artigo 4º, "os depoimentos pessoais, a oitiva

[202] Eis alguns dos incisos do artigo 7º, Resolução CNJ n. 354/2020, que sinalizam certo caráter protetivo ao fluxo de dados envolvidos na prática de atos processuais: "III – quando o ofendido ou testemunha manifestar desejo de depor sem a presença de uma das partes do processo, na forma da legislação pertinente, **a imagem poderá ser desfocada, desviada ou inabilitada,** sem prejuízo da possibilidade de transferência para lobby ou ambiente virtual similar; **IV – as oitivas telepresenciais ou por videoconferência serão gravadas, devendo o arquivo audiovisual ser juntado aos autos ou disponibilizado em repositório oficial de mídias indicado pelo CNJ (PJe Mídia) ou pelo tribunal; V– a publicidade será assegurada, ressalvados os casos de segredo de justiça**, por transmissão em tempo real ou por meio hábil que possibilite **o acompanhamento** por terceiros estranhos ao feito, ainda que mediante a exigência de prévio cadastro;"

de testemunhas, a acareação e o depoimento dos auxiliares do juízo prestados fora da sede do juízo serão tomados por videoconferência, somente utilizando-se de outro meio quando não houver condições para tanto". Tais depoimentos por videoconferência passam a ser prestados "na sala de audiências do Juízo deprecado, ou, se houver, em outra sala do fórum especialmente designada e preparada para este fim" (artigo 5º), sendo certo que a presença de magistrado na sala de audiência do juízo deprecado não é obrigatória, uma vez que a oitiva será presidida pelo juízo deprecante, devendo estar presente, a todo momento, um servidor indicado pelo juízo deprecado que acompanhará o ato (artigo 5º, § 2º). Na forma do artigo 7º, inciso VI, faz-se necessário que seja providenciado "o arquivamento de sons e imagens do(s) depoimento(s), facultada sua redução a termo, devendo o arquivo audiovisual ser juntado aos autos ou disponibilizado em repositório oficial de mídias indicado pelo CNJ (PJe Mídia) ou pelo tribunal", tudo a denotar que a questão da proteção de dados, também aqui, merece atenção.

Por fim, não é demasiado destacar que o princípio da concentração dos atos processuais e da informalidade que permeia o processo do trabalho pode levar a situações que ensejem análise imediata acerca do compartilhamento de atos concernentes às provas digitais, reavivando, também aqui, o debate em relação à presunção de consentimento que tradicionalmente é identificada com as fontes abertas em mídias sociais e a sua ausência em relação às fontes fechadas, por exemplo, com a sua compatibilização em relação ao interesse público e à autodeterminação informativa que permeia os dados pessoais, sobretudo os sensíveis, de terceiros que venham a fazer parte do fluxo de informações manejado no processo.[203] Sem dúvida, um assunto que ainda

[203] "Fontes fechadas são aquelas que não estão disponíveis ao público de maneira irrestrita, cujo acesso depende de algum tipo de credenciamento ou autorização. Como exemplos de fontes fechadas de informação, temos as informações relativas a sigilo fiscal ou bancário, interceptações telefônicas ou ambientais, para as quais exige-se autorização judicial, bem como aquelas informações constantes em bancos de dados que exijam algum tipo de credenciamento/obstáculo de acesso, como *login* e senha.
Fontes abertas, por outro lado, são aquelas disponíveis ao público e que não exigem credenciamento ou restrição para seu acesso, a exemplo de jornais, revistas, periódicos acadêmicos, livros e, de maneira mais pronunciada, dados disponíveis na Internet. O processo de obtenção de dados em fontes abertas que sejam úteis para a apuração dos fatos é conhecido como inteligência em fontes abertas (*Open Source Inteligence – OSINT)"*. CAVALCANTI, Gustavo. **Validade jurídica das provas digitais no processo administrativo disciplinar**. Distrito Federal: CGU, 2018. Disponível em:

merecerá, por parte do operador do direito, o devido aprofundamento e o adequado diálogo constitucional e institucional.

CONSIDERAÇÕES FINAIS

A circulação de dados por meio de processos automatizados no Poder Judiciário já havia sido incorporada ao cotidiano dos atos processuais por meio da Lei n. 11.419/2006. Com o processo judicial eletrônico, os magistrados e os operadores do direito passaram a conviver com linguagens não jurídicas e novas ferramentas tecnológicas capazes de traduzir, em algoritmos, *softwares* e recursos de mídias, o que se traduziu na necessidade de se repensar, ainda, a maneira com que o Poder Judiciário iria lidar com tais dados.

O contexto da pandemia do Covid-19 acelerou a incorporação de ferramentas tecnológicas ao cotidiano da prática de atos processuais, ao mesmo tempo em que intensificou a necessidade de atenção ao tratamento concedido aos dados tratados pelo fluxo sistematizado por tais ferramentas. Sob tal prisma, a Lei Geral de Proteção de Dados iniciou sua vigência com um modelo inspirado no sistema europeu de proteção, trazendo, contudo, nuances de maior amplitude e abrangência em seu texto legal.

Calcada em direitos fundamentais do titular dos dados, e em observância a princípios como a autodeterminação informativa, a transparência, a necessidade e a adequação voltadas ao interesse público, a Lei 13.709/20 trouxe arcabouço protetivo que merece ser analisado com profundidade, considerando-se as nuances e as prerrogativas da atividade jurisdicional, as inovações trazidas pelo cotidiano virtual incorporado às práticas processuais e, principalmente no caso do processo do trabalho, suas peculiaridades. Atento a tais características, certamente o Poder Judiciário, sem perder de vista o exercício de seu livre convencimento e independência, tornará mais profícua e dotada de efetividade a realidade desses novos tempos virtuais.

---

https://repositorio.cgu.gov.br/handle/1/31038#:~:text=Conclui%2Dse%20que%20os%20documentos,e%20f%C3%A9%20p%C3%BAblica%20do%20conte%C3%BAdo. Acesso em: 2 ago. 2021.

REFERÊNCIAS

ALLEN, Anita L. *Natural Law, Slavery, and the Right to Privacy Tort.* **Fordham L. Review**, v. 81, Issue 3, 2013. Disponível em: https://ir.lawnet.fordham.edu/flr/vol81/iss3/8. Acesso em: 5 ago. 2021.

BRANDEIS, Louis D. The right to privacy. **Harvard Law Review**, v. 4, n. 5, p. 193-220, dez. 1890.

CAVALCANTI, Gustavo. **Validade jurídica das provas digitais no processo administrativo disciplinar**. Distrito Federal: CGU, 2018. Disponível em: https://repositorio.cgu.gov.br/handle/1/31038#:~:text=Conclui%2Dse%20que%20os%20documentos,e%20f%C3%A9%20p%C3%BAblica%20do%20conte%C3%BAdo. Acesso em: 2 ago. 2021.

FERREIRA, Rafael Fonseca. Jurisdição 4.0 e inteligência artificial exegética: os novos "códigos". **Conjur**. 2019. Disponível em: https://www.conjur.com.br/2019-abr-20/diario-classe-jurisdicao-40-inteligencia-artificial-exegetica-novos-codigos. Acesso em: 25 ago. 2021.

HILBERT, Martin; LOPEZ, Priscila. The world's technological capacity to store, communicate, and compute information. ***Science****, v. 332, n. 6025, p. 60-65, 2011. Disponível em:* www.sciencemag.org. Acesso em: 18 ago. 2021.

KIM, Tae. Rosenbach v. Six Flags: Illinois Supreme Court Interprets Illinois Biometric Privacy Law. *In*: **Harvard Journal of Law & Technology – Jolt Digest**. Boston, 2019. Disponível em: https://jolt.law.harvard.edu/digest/rosenbach-v-six-flags-illinois-supreme-court-interprets-illinois-biometric-privacy-law. Acesso em: 3 set. 2021.

KORNSTEIN, Daniel J. The Roberson Privacy Controversy. **The Historical Society of the Courts of the State of New York**, Issue 4, 2006. Disponível

em: https://www.nycourts.gov/history/programs-events/images/Judicial-Notice-Newsletter-04.pdf. Acesso em: 4 ago. 2021.

LANEY, Doug B. **Infonomics***:* how to monetize, manage, and measure information as an asset for competitive advantage. *Routledge: Abingdon, 2017.*

MENKE, Fabiano. A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: **RJLB**, ano 5, n. 1, p. 781-809, 2019. Disponível em: http://www.cidp.pt/revistas/rjlb/2019/1/2019_01_0781_0809.pdf. Acesso em: 10 set. 2021.

ROTHMAN, Jennifer. **The right of publicity: privacy reimagined for a public world**. Boston: Harvard University Press, 2018.

SILVA, Thiago Rodrigo G. A privacidade, a proteção de dados e o direito de família. **Legale Scientia,** UNIMES, ed. especial, p. 94-99, 2021. Disponível em: https://periodicos.unimesvirtual.com.br/index.php/direito. Acesso em: 29 ago. 2021.

SIVOLELLA, Roberta Ferme. A aplicação supletiva e subsidiária do novo CPC – distinções: ...por uma visão dialógica da subsidiariedade e supletividade do Novo CPC frente à CLT: processualismo e argumentação. *In: BELMONTE, Alexandre Agra; DUARTE NETO, Bento Herculano; FREIRE e SILVA, Bruno* (coord.). ***O novo CPC aplicado ao processo do trabalho****.* São Paulo: LTr, 2016.

WINNICOTT, Donald. Freedom. **Nouv. Rev. Psychanal**., 1986, p. 228-238.