LEI GERAL DE PROTEÇÃO DE DADOS APLICADA PELOS TRIBUNAIS TRABALHISTAS: A COLETA DE DADOS PELO PODER JUDICIÁRIO E A COLISÃO DE PRINCÍPIOS

GENERAL DATA PROTECTION LAW APPLIED BY LABOR COURTS: THE COLLECTION OF DATA BY THE JUDICIARY AND THE COLLISION OF PRINCIPLES

Bruna de Sá Araújo*

Luciana Lara Sena Lima**

RESUMO: O presente artigo tem por objetivo analisar o impacto da Lei Geral de Proteção de Dados nos Tribunais Trabalhistas brasileiros em razão de dois motivos: a LGPD aplica-se às pessoas jurídicas de direito público e esses órgãos do Judiciário são detentores de uma imensidão de dados pessoais e sensíveis. Em plena vigência desde o dia 18 de setembro de 2020, faz-se necessário discutir e regularizar problemáticas que surgem da aplicação da LGPD pelos órgãos Judiciários e a colisão de princípios desencadeada pela norma. A partir de tais análises e adotando uma abordagem qualitativa e exploratória, conclui-se que a Lei francesa nº 2019-222 pode ser um exemplo de possível solução para a colisão entre os princípios da publicidade e da transparência e o princípio da privacidade. Por conseguinte, a retirada dos nomes e sobrenomes das pessoas físicas e a omissão dos dados quando for suscetível de prejudicar a segurança ou o respeito da privacidade das partes ou sua comitiva, podem ser exemplos a serem seguidos pelo Judiciário brasileiro.

PALAVRAS-CHAVE: LGPD. Dados Pessoais. Dados Pessoais Sensíveis. Proteção de Dados. Princípio da Privacidade.

ABSTRACT: The purpose of this paper's to analyze the impact of the General Data Protection Law on Brazilian labor courts for two reasons: the LGPD applies to legal entities governed by public law and these bodies of the Judiciary are holders of an immensity of personal data and sensitive. In full force since September 18, 2020, it is necessary to discuss and regularize issues that arise from the application of LGPD by Organs Judiciary bodies and the collision of principles triggered by the rule. From such analyzes and adopting a qualitative and exploratory approach, it is concluded that French Law no. 2019-222 can be an example of a possible solution to the collision

* *MBA em Ciências e Legislação do Trabalho pelo IPOG; especialista em Direito do Trabalho e Processo do Trabalho pela Universidade Federal de Goiás (UFG); pós-graduanda em Direito Previdenciário pela Faculdade Sul Americana (FASAM); coordenadora do Núcleo de Direito do Trabalho do Instituto de Estudos Avançados em Direito (IEAD).*

** *Mestra em Direito, Relações Internacionais e Desenvolvimento pela Pontifícia Universidade Católica de Goiás (2015); doutoranda em Ciências Jurídicas pela Universidade Autônoma de Lisboa (UAL); conselheira seccional da OAB Goiás (2019/2021); diretora adjunta na ESA Goiás (2019/2021).*

between the principles of advertising and transparency and the principle of privacy. Consequently, the removal of the names and surnames of individuals and the omission of data when it is likely to jeopardize the security or respect of the privacy of the parties or their entourage, can be examples to be followed by the Brazilian Judiciary.

KEYWORDS: LGPD. Personal Data. Sensitive Personal Data. Data Protection. Principle of Privacy.

1 – Introdução

Há tempos a proteção de dados já era discutida e regulamentada em outros países, a Declaração da ONU dos Direitos Humanos (1948) e a Declaração Europeia dos Direitos do Homem (1950) são consideradas as primeiras declarações internacionais subscritas por países europeus que mencionam a privacidade e o direito à sua proteção.

No Brasil, a Lei nº 12.965/2014 (Marco Civil da Internet) é considerada a primeira legislação a dispor expressamente sobre a questão dos dados pessoais, ao tratar temas como neutralidade da rede, retenção de dados e funções sociais da internet, como liberdade de expressão, transmissão de conhecimento e responsabilidade civil.

Contudo, recentemente passou a viger no país lei mais específica e aprofundada sobre o tema da proteção de dados; trata-se da Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018[1], com as alterações promovidas pela Lei nº 13.853/2019, que dispõe sobre a proteção de dados pessoais.

A LGPD pretende preservar o direito constitucional à liberdade e à privacidade que todos os cidadãos brasileiros têm, assim como protegê-los de danos causados por rupturas desses direitos. O art. 1º prevê que a sua aplicação também abarca as "pessoas jurídicas de direito público". Dessa forma, urge discutir e regulamentar o alcance dessa diretriz às publicações de dados realizadas pelos Tribunais Trabalhistas, órgãos que detêm uma enorme quantidade de dados de pessoas físicas e jurídicas.

Com a implantação e expansão do Processo Judicial Eletrônico (PJe) em meados de 2010, o Judiciário passou a gerir uma quantidade colossal de dados pessoais e sensíveis de diversos cidadãos jurisdicionados. Assim, considerando que o Poder Judiciário, como parte do Estado, é guardião de dados, discute-se no presente artigo se essa publicidade e transparência não colidiriam com as diretrizes da LGPD e com o princípio da privacidade.

---

1 BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 10 set. 2020.

A título exemplificativo, basta considerar que os dados de diversos reclamantes que obtêm êxito na Justiça do Trabalho são divulgados em bancos públicos de jurisprudência, *sites* de notícias jurídicas e, às vezes, no próprio tribunal em que sua ação foi ajuizada, acarretando uma exposição e risco à segurança do autor.

Uma solução para a colisão entre os princípios da publicidade e da transparência e o princípio da privacidade seria o exemplo visualizado na Lei francesa nº 2019-222. A retirada dos nomes e sobrenomes das pessoas físicas e a omissão dos dados quando for suscetível de prejudicar a segurança ou o respeito da privacidade das partes ou sua comitiva podem ser exemplos a serem seguidos pelo Judiciário brasileiro.

Com a LGPD em plena vigência no Brasil desde 18 de setembro de 2020, é salutar discutir e regularizar pontas soltas deixadas pela legislação específica. Tendo em vista o armazenamento de milhares de dados nos *sites* dos Tribunais no Brasil, muitas vezes replicados em bancos públicos de jurisprudência e *sites* de notícias jurídicas, urge definir a responsabilidade dos Tribunais, em especial os Regionais e Tribunal Superior do Trabalho, no tocante à proteção de dados.

Dessa maneira, o presente artigo buscou analisar as primeiras regulamentações sobre a proteção de dados no Brasil e no mundo, demonstrar como a divulgação de dados pelos Tribunais brasileiros enseja uma verdadeira colisão de princípios – princípio da publicidade e da transparência x princípio da proteção e da privacidade, por fim, indica a Lei francesa nº 2019-222 como possível solução para esse impasse.

2 – As primeiras regulamentações sobre a proteção de dados no mundo

A Declaração da ONU dos Direitos Humanos[2] (1948) e a Declaração Europeia dos Direitos do Homem[3] (1950) são consideradas as primeiras declarações internacionais subscritas por países europeus que mencionam a privacidade e o direito à proteção. No entanto, tratavam de maneira vaga e superficial sobre a proteção dos dados pessoais.

Por outro lado, a Convenção nº 108 do Conselho da Europa[4] estabeleceu a proteção de indivíduos quanto ao processamento automático de tratamento de dados, objetivando instituir métodos mais criteriosos como a previsão das

2 Disponível em: https://nacoesunidas.org/direitoshumanos/declaracao/. Acesso em: 10 set. 2020.

3 Disponível em: https://www.echr.coe.int/Documents/Convention_POR.pdf. Acesso em: 10 set. 2020.

4 Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37. Acesso em: 10 set. 2020.

"garantias relativas à coleta e tratamento de dados pessoais". Assim, a referida convenção proíbe,

> "na ausência de garantias jurídicas adequadas, o tratamento de dados 'sensíveis', tais como dados sobre a raça, a opinião política, a saúde, as convicções religiosas, a vida sexual ou o registo criminal de uma pessoa."

No ano de 1995, com o objetivo de aperfeiçoar e dar efetividade à Convenção nº 108, a União Europeia promulgou a Diretiva nº 95/46/CE[5], que pretendia estabelecer, harmonizar e promover igualdade no tratamento de dados pessoais pelos Estados-Membros. Por se tratar de uma diretiva, seria necessário que cada Estado adotasse o texto comunitário em seu direito interno, o que ensejou diferentes níveis de proteção em cada um dos países europeus.

No entanto, o Regulamento (UE) nº 2.016/679 do Parlamento Europeu e do Conselho[6], relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, decidiu revogar a Diretiva nº 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

Dois anos mais tarde, o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia, com 11 capítulos e 99 artigos, entrou em vigor, atualizando, harmonizando e adaptando a antiga Diretiva Europeia de Proteção de Dados às mais novas formas de uso massivo de dados pessoais, tais como os modelos de negócio baseados em tecnologias de *big data*, inteligência artificial e aprendizado de máquina. O regulamento estabelecia as regras relativas ao tratamento, por uma pessoa, uma empresa ou uma organização, de dados pessoais relativos a pessoas.

Nos artigos 4º, itens 13, 14 e 15, e 9º, além dos Considerandos 51 a 56 do GDPR, há previsão sobre os denominados dados sensíveis, que são os dados pessoais que revelem origem racial ou étnica, opiniões políticas e convicções religiosas ou filosóficas; filiação sindical; dados genéticos, dados biométricos tratados simplesmente para identificar um ser humano; dados relacionados com a saúde; dados relativos à vida sexual ou à orientação sexual da pessoa.

Em relação ao tratamento de dados, o artigo 4º, itens 2 e 6, da GDPR inclui o recolhimento, o registro, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por

5 Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 10 set. 2020.

6 Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679. Acesso em: 10 set. 2020.

transmissão, difusão ou qualquer outra forma de disponibilização, comparação ou interconexão, a limitação, o pagamento ou a destruição de dados pessoais. Tal previsão é aplicável ao tratamento dos dados pessoais, seja por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em arquivos (ficheiros).

Na Alemanha, pode-se citar a Lei Federal de Proteção de Dados de 2017 (Bundesdatenschutzgesetz – BDSG)[7], que segue os preceitos da GDPR e pretendeu substituir a lei de mesmo nome que havia sido instituída em 2001. A BDSG trata dos direitos e deveres de órgãos públicos e privados para as atividades de coleta e processamento de dados, que têm o dever de contratar um profissional responsável por privacidade de dados e de determinar regras claras para avaliações de *score* de crédito, por exemplo. Além disso, há diretrizes específicas para como as empresas devem e podem fazer tratamentos de dados de seus funcionários.

A Lei de Proteção de Dados da Argentina (Lei nº 25.326)[8] determinou que a coleta de dados só poderá ser feita mediante o consentimento do usuário. A lei, que se aplica a qualquer pessoa ou entidade que lida com dados pessoais no país, dispõe ainda que o titular dos dados (o indivíduo a quem as informações se referem) tem o direito de acessar, corrigir, deletar e solicitar a exclusão de seus dados.

Na Austrália, as matérias relativas à segurança e proteção de dados são regidas pela Lei de Privacidade de 1988[9], que governa tanto as instituições do setor público quanto as do setor privado. A lei foi redigida com base nos 13 Princípios Australianos de Privacidade (APPs, ou *Australian Privacy Principles*)[10], que discorrem sobre temas como uso e divulgação de dados; direitos do titular dos dados; manutenção da qualidade dos dados; e transparência e anonimidade. Ademais, a lei é complementada pelas regulamentações estaduais de privacidade e pelas leis de proteção de dados, direcionadas para setores específicos, estabelecidas de acordo com o uso que cada mercado faz de dados pessoais.

O Canadá possui um total de 28 regulamentações, entre leis provinciais e federais, que tratam das questões relativas à privacidade e proteção de da-

7 Disponível em: https://www.gesetze-im-internet.de/bdsg_2018/. Acesso em: 10 set. 2020.

8 Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm. Acesso em: 10 set. 2020.

9 Disponível em: http://www6.austlii.edu.au/cgi-bin/viewdb/au/legis/cth/consol_act/pa1988108/. Acesso em: 10 set. 2020.

10 Disponível em: https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-quick-reference/. Acesso em: 10 set. 2020.

dos. A legislação nacional referente a isso é a PIPEDA (*Personal Information Protection and Electronic Documents Act*, ou "Lei de Proteção de Informações Pessoais e Documentos Eletrônicos")[11]. Aplicável em todas as províncias do Canadá, a PIPEDA apresenta diretrizes referentes à coleta, tratamento e divulgação de dados pessoais coletados por empresas durante o exercício de suas atividades comerciais, assim como para transferências internacionais e interregionais de dados pessoais.

A PIPEDA opera sobre dez princípios basilares de boas práticas a serem seguidos pelas empresas (bastante similares às bases da LGPD brasileira), são eles:

1. as empresas são responsáveis pelos dados pessoais que coletaram e que usam;

2. é preciso identificar claramente os propósitos por trás de uma coleta de dados;

3. é preciso ter o consentimento do titular para coleta, uso e compartilhamento de seus dados, salvo exceções previstas por lei;

4. podem ser coletados somente os dados necessários dentro do propósito informado;

5. os dados solicitados podem ser usados, divulgados e mantidos pela empresa apenas da maneira informada e enquanto cumprirem os propósitos;

6. as informações pessoais devem ser verídicas e mantidas atualizadas;

7. os dados devem ser protegidos sob medidas adequadas de acordo com a sensibilidade das informações;

8. a organização precisa fornecer amplamente informações claras e detalhadas sobre suas políticas e práticas de segurança e proteção de dados;

9. o titular dos dados tem o direito de receber informações sobre a existência de tratamentos de suas informações, assim como questionar se seus dados são verídicos e estão completos;

10. o titular dos dados tem o direito de questionar as organizações que tratam e coletam suas informações pessoais, dentro dos nove princípios anteriores.

Já no continente asiático, a mais recente regulamentação chinesa sobre privacidade é a Lei de Tecnologia da Informação: Especificação Sobre Segurança de Informações Pessoais (GB/T 35273-2017)[12]. Denominada de "O

11 Disponível em: https://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html. Acesso em: 10 set. 2020.

12 Disponível em: http://pip.tc260.org.cn/assets/wz/2020-03-07/ef2dab88-cd9d-4748-814a-a3eca027beba.pdf. Acesso em: 10 set. 2020.

Padrão", a regulamentação traz diretrizes sobre transparência, direitos do titular e consentimento quanto ao tratamento de dados pessoais.

Antes da entrada em vigência da Lei GB/T 35273-2017, o conjunto de regras chinesas sobre o tema era pulverizado por diferentes regulamentações, como a Lei Civil da República Popular da China (de 2017), a Lei de Cibersegurança (2017), a Lei Criminal (2015), a Decisão de Fortalecer a Proteção das Redes de Informações (2012), o Padrão Nacional de Segurança da Tecnologia da Informação (2013) e a Lei de Proteção ao Consumidor (2014).

No Japão, até 2003 a proteção de dados era regulada pela Lei de Proteção de Informações Pessoais (Lei nº 57, de 2003)[13]. Posteriormente, o Japão colocou em prática a chamada Emenda APPI de 2017[14], que traz preceitos básicos para a proteção de dados pessoais. A Emenda APPI dispõe regras sobre compartilhamento de dados com terceiros, manutenção de informações em bancos de dados, anonimização de dados e vazamentos, estabelecendo diretrizes para proteger os titulares.

3 – A regulamentação da proteção de dados no Brasil

Sem especificar a questão relacionada à proteção de dados, a Constituição da República Federativa do Brasil traz no *caput* do art. 5º a proteção à segurança de brasileiros e estrangeiros residentes no país. Considerando os direitos fundamentais sob uma ótica expansionista, também poderia ser incluída nesse conceito a proteção de dados.

O inciso X do referido artigo dispõe que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas (...)". Ainda sob um viés expansionista protetivo, o direito à privacidade também se relaciona diretamente com a proteção de dados.

Outra importante legislação sobre o tema no país é o Marco Civil da Internet (Lei nº 12.965), sancionado em 2014[15]. Voltado inteiramente para o uso da internet no país, o Marco Civil traz princípios, garantias, direitos e deveres dos usuários da rede, além de diretrizes sobre como o Estado deve atuar. Ao

13 Disponível em: http://www.japaneselawtranslation.go.jp/law/detail_main?re=02&ia=03&vm=02&id=2781. Acesso em: 10 set. 2020.

14 Disponível em: https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf. Acesso em: 10 set. 2020.

15 BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. (Marco Civil da Internet). Disponível em: https://legislacao.presidencia.gov.br/atos/?tipo=LEI&numero=12965&ano=2014&ato=93eUTRE9ENVpWTdb6. Acesso em: 10 set. 2020.

lado da privacidade, alguns dos outros principais temas abordados pela lei são: neutralidade da rede, retenção de dados e funções sociais da internet, como liberdade de expressão, transmissão de conhecimento e responsabilidade civil.

O princípio da privacidade é conceituado como a garantia de inviolabilidade das comunicações dos usuários. Nesse contexto, a Lei do Marco Civil atribui o dever de sigilo de suas informações ao provedor do recurso de internet. A isenção de tal garantia pode acontecer somente por meio de ordem judicial, quando forem imprescindíveis para a elucidação de ações ilícitas, bem como na tentativa de identificação dos seus responsáveis.

A lei mais específica e aprofundada sobre o tema da proteção de dados é a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018[16], com as alterações promovidas pela Lei nº 13.853/2019, que dispõe sobre a proteção de dados pessoais. A LGPD entrou em vigor no dia 18 de setembro de 2020, após o presidente Jair Bolsonaro sancionar o Projeto de Lei de Conversão nº 34/2020, originado da Medida Provisória nº 959/2020.

Ao editar a MP, em abril de 2020, o governo incluiu, em seu art. 4º, um dispositivo que previa o adiamento da entrada em vigor da LGPD, para maio de 2021. Como tem força de lei, assim que foi publicada a MP, a vigência da LGPD foi adiada. Contudo, ao passar pela análise do Congresso Nacional, o dispositivo em comento não foi aprovado.

A LGPD visa preservar o direito constitucional à liberdade e à privacidade que todos os cidadãos brasileiros têm, assim como protegê-los de danos causados por rupturas desses direitos. A LGPD se aplica a qualquer tratamento de dados ocorrido (total ou parcialmente) em solo brasileiro, ou que tenha por objetivo vender produtos e serviços nacionais. Além disso, a lei é voltada para tratamentos com fins comerciais, ou seja, trocas e outros tratamentos de dados entre pessoas físicas sem objetivos de compra ou venda de produtos e serviços não se enquadram.

A lei esclarece que o direito à privacidade e à liberdade não impede a coleta, o uso e outros tratamentos de dados para fins jornalísticos, artísticos ou acadêmicos. Dessa forma, preserva-se a liberdade de imprensa, da arte e da ciência[17].

---

16 BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 10 set. 2020.

17 Disponível em: https://guialgpd.com.br/lgpd-comentada/. Acesso em: 10 set. 2020.

O art. 5º é considerado um dos mais importantes da lei, pois estabelece a definição de conceitos fundamentais básicos para a compreensão do texto como um todo, tais como dado pessoal, dado pessoal sensível, dado anonimizado, banco de dados, titular, controlador, operador, encarregado, agentes de tratamento, tratamento, anonimização, consentimento, bloqueio, eliminação, transferência internacional de dados, uso compartilhado de dados, relatório de impacto à proteção de dados pessoais, órgão de pesquisa e autoridade nacional.

A lei ainda traz a determinação de que o titular tem direito de solicitar informações sobre a finalidade, a duração e a forma de tratamento dos dados, assim como saber se seus dados estão sendo ou foram compartilhados com outros agentes.

4 – A aplicação da LGPD pelos tribunais trabalhistas

4.1 – A divulgação de dados pessoais pelos tribunais brasileiros e a colisão de princípios

Antes da difusão da internet, no final da década de 1980, a coleta de dados era mais trabalhosa, uma vez que o Poder Judiciário e os operadores do Direito produziam documentos físicos e inexistiam métodos acessíveis de análise, organização e classificação de dados. Atualmente, com o advento da quarta revolução industrial e a informatização de quase todo o sistema processual brasileiro, além da obrigatoriedade legal de publicidade da quase totalidade dos processos, acarretou-se uma grande quantidade de dados gerados pelo Judiciário, consolidados nas versões *online* dos diários oficiais ou nos próprios *sites* dos Tribunais.

Um *software* que funcionasse como um sistema único de tramitação eletrônica de processos judiciais já era idealizado por cinco Tribunais Regionais Federais e pelo Conselho da Justiça Federal, contudo, o projeto só foi iniciado em setembro de 2009, pelo Conselho Nacional de Justiça (CNJ).

Em 29 de março de 2010, por ocasião da celebração do Termo de Acordo de Cooperação Técnica nº 51/2010 entre o Conselho Nacional de Justiça (CNJ), o Tribunal Superior do Trabalho (TST) e o Conselho Superior da Justiça do Trabalho (CSJT), a Justiça do Trabalho aderiu, oficialmente, ao Processo Judicial Eletrônico – PJe. Na mesma data, por meio do Acordo de Cooperação Técnica nº 01/2010, assinado entre o Tribunal Superior do Trabalho, o Conselho

Superior da Justiça do Trabalho e os 24 Tribunais Regionais do Trabalho de todo o país, todos os órgãos da Justiça do Trabalho passaram a integrar o projeto[18].

Com o PJe, o Judiciário Trabalhista teve a possibilidade de alterar a estrutura do procedimento judicial, automatizar a prática de inúmeros atos e se modernizar, acompanhando as inovações e avanços do universo tecnológico, bem como a difusão e acessibilidade do uso da internet[19].

Não obstante, ao disponibilizar essa grande quantidade de dados, inclusive os chamados dados sensíveis e os dados pessoais, indaga-se se o Poder Judiciário não estaria infringindo as normativas nacionais e internacionais mencionadas alhures sobre proteção de dados.

A indagação e sua resposta são preocupantes, uma vez que o Poder Judiciário, como parte do Estado e guardião de dados sensíveis e pessoais de inúmeros cidadãos jurisdicionados, não poderia disponibilizar tais dados, sem limites claros e restritivos dispostos na legislação aplicável.

É cediço que no Brasil os processos e seu conteúdo são públicos, com exceção dos processos que tramitam em segredo de justiça. Sem assinatura eletrônica dos procuradores ou membros do Judiciário, não é possível que o cidadão comum consiga ler o teor dos autos eletrônicos se não for parte envolvida e possuir a senha de acesso.

Por outro lado, é notório que a jurisprudência e as decisões ficam disponíveis no Diário Oficial e banco de decisões do Tribunal, de modo que inúmeros dados pessoais e dados pessoais sensíveis ficam disponíveis ao público em geral, violando o direito à privacidade e proteção de dados de diversos cidadãos.

Basta imaginar situações em que um reclamante obtém êxito na sua reclamação trabalhista e aufere uma grande quantia na condenação, muitas vezes valores milionários. Seu nome completo e dados pessoais sensíveis podem ser facilmente encontrados no *site* do Tribunal Trabalhista em que correu sua ação ou bancos públicos de jurisprudência. Além da divulgação de dados, uma simples consulta ao processo também permite visualizar o estágio da tramitação, bem como se o alvará já foi expedido.

Outras vezes, também ocorre de o resultado da ação ser amplamente divulgado em mídias sociais e *sites* de notícias jurídicas, *site* profissional do advogado atuante, ou até mesmo no campo "Notícias" no *site* do próprio Tribunal.

18 BRASIL. Tribunal Superior do Trabalho. *Histórico do PJE*. Disponível em: http://www.tst.jus.br/web/pje/historico. Acesso em: 17 jul. 2020.

19 ARAÚJO, Bruna de Sá. PJE. *Revista Eletrônica do Tribunal Regional do Trabalho da 9ª Região*, Paraná, v. 9, p. 25-31, jul. 2020.

Além da exposição pública e risco à própria vida, dada a possibilidade de ocorrerem sequestros ou assaltos do reclamante ou de pessoas próximas, há também uma violação ao direito à privacidade, segurança e intimidade dos cidadãos jurisdicionados.

Conforme advertido por Marcelo Novelino[20], no Estado Democrático de Direito, os princípios, diferentemente das regras, devem ter aplicação mitigada quando verificada contraposição. Considerando os princípios que balizam a Lei de Acesso à Informação, Política de Dados abertos, Controle Social e a Lei de Proteção de Dados Pessoais, imprescindível observar o alcance e aplicação de cada um.

Assim, partindo de uma análise de princípios em colisão, é preciso analisar qual deles merece maior proteção, o princípio da publicidade e da transparência ou o princípio da privacidade? O Poder Judiciário deve seguir disponibilizando a sua base de dados dos processos e dos julgamentos de forma integral e gratuita?

Deveras, a LGPD também é aplicada no setor público, haja vista a expressa menção no art. 1º de que a sua aplicação também envolve as "pessoas jurídicas de público". Dessa forma, urge discutir e regulamentar o alcance dessa diretriz às publicações de dados realizadas pelos Tribunais Trabalhistas, órgãos que detêm uma enorme quantidade de dados de pessoas físicas e jurídicas.

4.2 – O que os tribunais brasileiros podem aprender com a Lei francesa nº 2019-222 e a proteção de dados na França

No dia 23 de março de 2019, a Assembleia Nacional da França promulgou a Lei nº 2019-222, que trata da programação judiciária do país até 2022 e promove uma ampla reforma na justiça, incluindo diversas alterações em artigos do Código Civil, Comercial, Eleitoral, de Saúde Pública, dentre outros. A partir desse objetivo geral, a lei aproveitou a oportunidade para regulamentar o acesso aos dados judiciários[21].

Assim, a partir de 2019, a França proibiu a divulgação de estatísticas sobre decisões judiciais, consoante a regra do artigo 33 da referida Lei francesa, que também adicionou dispositivos a outras leis, como o Código Penal. O artigo 33 estabelece

20 NOVELINO, Marcelo. *Direito constitucional*. 2. ed. São Paulo: Método, 2008. p. 65-66.

21 CORRÊA, Fernando; TRECENTI, Julio; NUNES, Marcelo Guedes. *A lei francesa de acesso a dados judiciários*: algumas reflexões. Disponível em: https://www.migalhas.com.br/depeso/304441/a-lei-francesa-de-acesso-a-dados-judiciarios-algumas-reflexoes. Acesso em: 10 set. 2020.

> "(...) que os dados de identidade de magistrados e servidores do Judiciário não podem ser reutilizados com o objetivo ou efeito de avaliar, analisar, comparar ou prever suas práticas profissionais, reais ou supostas."

O artigo 33 (V) da Lei nº 2013-111, que foi modificado pela Lei nº 2019-222, determina que as decisões dos tribunais judiciais são disponibilizadas gratuitamente ao público em formato eletrônico, mas sujeitos às disposições especiais que regem o acesso e a publicidade das decisões judiciais: os nomes e sobrenomes das pessoas singulares mencionadas na decisão, quando são partes ou terceiros, ficam ocultos antes da disponibilização ao público. O artigo também prevê que, quando a divulgação dos dados for suscetível de prejudicar a segurança ou o respeito da privacidade dessas pessoas ou sua comitiva, também estará oculto qualquer elemento que permita identificar as partes, os terceiros, os magistrados e os membros do registro.

A violação da proibição à predição é punida com as penalidades previstas nos artigos 226-18, 226-24 e 226-31 do Código Penal, que podem chegar à pena máxima de cinco anos de reclusão, sem prejuízo das medidas e sanções previstas pela Lei nº 78-17, de 6 de janeiro de 1978, relativa ao tratamento de dados, arquivos e liberdades.

A premissa da qual a lei parte é que, ao restringir o acesso a dados pessoais e liberar o acesso aos dados de conteúdo, a justiça francesa estaria conciliando a publicidade das informações jurídicas com a proteção à intimidade das pessoas envolvidas[22].

A vedação dos tratamentos ligados à identidade dos magistrados é justificada pelo argumento de que a construção de perfis individualizados é contrária ao funcionamento adequado da justiça. Parlamentares franceses impugnaram a vedação no Conselho Constitucional francês, alegando que a proibição do tratamento desses dados violaria o princípio da igualdade, uma vez que a construção dos perfis contribuiria para o estabelecimento de uma "paridade de armas" entre litigantes[23].

No entanto, o argumento foi rejeitado pelo Conselho Constitucional francês, conforme a Decisão 2019-778 DC[24], na qual se afirmou que a predição dos magistrados contribuiria para pressionar a atuação do Poder Judiciário e para

22 *Ibid*.

23 ORSINI, Adriana Goulart de Sena. Jurimetria e predição: notas sobre uso dos algoritmos e o Poder Judiciário. In: *Futuro do trabalho*: efeitos da revolução digital na sociedade, Brasília: ESMPU, 2020. p. 326.

24 Disponível em: https://www.conseil-constitutionnel.fr/decision/2019/201977 8DC.htm. Acesso em: 10 set. 2020.

que as partes escolhessem estratégias de litigância em razão das características individuais dos magistrados, distorcendo o funcionamento da justiça francesa.

A retirada dos nomes e sobrenomes das pessoas físicas mencionadas nas decisões francesas a partir de 2019, independentemente do fato de serem partes ou terceiros, antes da disponibilização ao público, visa atender as determinações da GDPR. A Lei francesa levou em consideração o fato de que são dados sensíveis aqueles que não podem ser disponibilizados ao público, tratando-se de uma forma de proteção dos envolvidos.

Desse modo, a GDPR determina que, se a divulgação de outras informações colocar em risco a segurança ou o respeito pela vida privada dessas pessoas ou seus arredores, não deverão ser publicadas, assim como qualquer informação que identifique as partes ou terceiros.

O exemplo da legislação francesa poderia servir como exemplo para a proteção de dados pessoais e sensíveis de cidadãos brasileiros jurisdicionados. No entanto, a LGPD abriu exceções que podem prejudicar a segurança e privacidade da população do país.

Conforme se denota da leitura do art. 7º da LGPD, o consentimento é a base fundamental para diversos dos tratamentos de dados realizados pelos controladores. Não obstante, a LGPD prevê que o consentimento não é obrigatório em alguns casos.

Essa exceção vale para órgãos da Administração Pública quando o tratamento visar ao cumprimento de leis e de políticas públicas, como para a execução de contratos ou para o exercício regular de direitos, isto é, ao utilizar dados em uma ação judicial, por exemplo. Órgãos de pesquisa também não precisam exigir consentimento, mas devem trabalhar com dados anonimizados sempre que possível, assim, é possível ter acesso aos dados estatísticos sem que eles sejam conectados a um titular específico.

Alexandre de Morais[25] vaticina que os direitos fundamentais não podem ser analisados como absolutos e inflexíveis; havendo conflito entre eles, deverão ser interpretados para que haja a devida harmonia. Complementa que:

> "(...) quando houver conflito entre dois ou mais direitos ou garantias fundamentais, o intérprete deve utilizar-se do princípio da concordância prática ou da harmonização, de forma a coordenar e combinar os bens jurídicos em conflito, evitando o sacrifício total de uns em relação aos outros, realizando uma redução proporcional do âmbito de alcance

25 MORAES, Alexandre de. *Direito constitucional*. 32. ed. São Paulo: Atlas, 2016. p. 92.

de cada qual (contradição dos princípios), sempre em busca do verdadeiro significado da norma e da harmonia do texto constitucional com sua finalidade precípua."[26]

Uma solução para a colisão entre os princípios da publicidade e da transparência e o princípio da privacidade seria o exemplo visualizado na Lei francesa nº 2019-222. A retirada dos nomes e sobrenomes das pessoas físicas e a omissão dos dados quando for suscetível de prejudicar a segurança ou o respeito da privacidade das partes ou sua comitiva podem ser exemplos a serem seguidos pelo Judiciário brasileiro.

Com a LGPD em plena vigência no Brasil desde 18 de setembro de 2020, é salutar discutir e regularizar pontas soltas deixadas pela legislação específica. Tendo em vista o armazenamento de milhares de dados nos *sites* dos Tribunais no Brasil, muitas vezes replicados em bancos públicos de jurisprudência e *sites* de notícias jurídicas, impera definir a responsabilidade dos Tribunais, em especial os Regionais e Tribunal Superior do Trabalho, no tocante à proteção de dados.

5 – Considerações finais

Em plena vigência no Brasil desde o dia 18 de setembro de 2020, a Lei Geral de Proteção de Dados (LGPD) enseja ampla discussão sobre problemáticas oriundas da necessidade de proteção de dados. O presente artigo buscou discutir a questão que afeta os Tribunais trabalhistas do país, demonstrando que tais órgãos também precisam adequar-se à nova legislação que regula de forma específica a proteção de dados.

Partindo de um estudo aprofundado sobre as primeiras regulamentações sobre proteção de dados no mundo, demonstrou-se que o tema em questão foi discutido e regulado com maior profundidade em países da União Europeia, Ásia e América do Norte.

De maneira superficial, no Brasil, o art. 5º, *caput* e inciso X, da Constituição Federal prevê a proteção e inviolabilidade dos brasileiros e estrangeiros residentes no país, sem especificar se tal proteção abrangeria a proteção de dados. Em 2014, foi sancionada a Lei nº 12.965, chamada de Marco Civil da Internet, que dispõe sobre temas como neutralidade da rede, retenção de dados e funções sociais da internet, como liberdade de expressão, transmissão de conhecimento e responsabilidade civil.

A lei mais específica e aprofundada sobre o tema da proteção de dados é a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, com as al-

26 *Ibid*., p. 93.

terações promovidas pela Lei nº 13.853/2019, que dispõe sobre a proteção de dados pessoais. A LGPD visa preservar o direito constitucional à liberdade e à privacidade que todos os cidadãos brasileiros têm, assim como protegê-los de danos causados por rupturas desses direitos.

As inovações tecnológicas permitiram a informatização de quase todo o sistema processual brasileiro e ampliou a publicidade das decisões judiciais. Soma-se a isso a grande quantidade de dados gerados pelo Judiciário, consolidados nas versões *online* dos diários oficiais ou nos próprios *sites* dos tribunais.

Ao disponibilizar essa grande quantidade de dados, inclusive os chamados dados sensíveis e os dados pessoais, o artigo buscou discutir se o Poder Judiciário não estaria infringindo as normativas nacionais e internacionais mencionadas alhures sobre proteção de dados.

Por fim, demonstrou-se que a Lei francesa nº 2019-222 pode ser um exemplo de possível solução para a colisão entre os princípios da publicidade e da transparência e o princípio da privacidade. Assim, a retirada dos nomes e sobrenomes das pessoas físicas e a omissão dos dados quando for suscetível de prejudicar a segurança ou o respeito da privacidade das partes ou sua comitiva podem ser exemplos a serem seguidos pelo Judiciário brasileiro.

6 – Referências bibliográficas

ARAÚJO, Bruna de Sá. PJE. *Revista Eletrônica do Tribunal Regional do Trabalho da 9ª Região*, Paraná, v. 9, p. 25-31, jul. 2020.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. (Marco Civil da Internet). Disponível em: https://legislacao.presidencia.gov.br/atos/?tipo=LEI&numero=12965&ano=2014&ato=93eUTRE9ENVpWTdb6. Acesso em: 10 set. 2020.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 10 set. 2020.

BRASIL. Tribunal Superior do Trabalho. *Histórico do PJE*. Disponível em: http://www.tst.jus.br/web/pje/historico. Acesso em: 17 jul. 2020.

CORRÊA, Fernando; TRECENTI, Julio; NUNES, Marcelo Guedes. *A lei francesa de acesso a dados judiciários*: algumas reflexões.

MORAES, Alexandre de. *Direito constitucional*. 32. ed. São Paulo: Atlas, 2016.

NOVELINO, Marcelo. *Direito constitucional*. 2. ed. São Paulo: Método, 2008.

ORSINI, Adriana Goulart de Sena. Jurimetria e predição: notas sobre uso dos algoritmos e o Poder Judiciário. In: *Futuro do trabalho*: efeitos da revolução digital na sociedade, Brasília: ESMPU, 2020.

Internet

A Declaração Universal dos Direitos Humanos. Disponível em: https://nacoesunidas.org/direitoshumanos/declaracao/. Acesso em: 10 set. 2020.

A lei francesa de acesso a dados judiciários: algumas reflexões. Disponível em: https://www.migalhas.com.br/depeso/304441/a-lei-francesa-de-acesso-a-dados-judiciarios-algumas-reflexoes. Acesso em: 10 set. 2020.

Act on the Protection of Personal Information. Disponível em: http://www.japaneselawtranslation.go.jp/law/detail_main?re=02&ia=03&vm=02&id=2781. Acesso em: 10 set. 2020.

Amended Act on the Protection of Personal Information. Disponível em: https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf. Acesso em: 10 set. 2020.

Atos Consolidados da Commonwealth. Disponível em: http://www6.austlii.edu.au/cgi-bin/viewdb/au/legis/cth/consol_act/pa1988108/. Acesso em: 10 set. 2020.

Convenção Europeia dos Direitos do Homem. Disponível em: https://www.echr.coe.int/Documents/Convention_POR.pdf. Acesso em: 10 set. 2020.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37. Acesso em: 10 set. 2020.

Décision nº 2019-778 DC. Disponível em: https://www.conseil-constitutionnel.fr/decision/2019/2019778DC.htm. Acesso em: 10 set. 2020.

Directiva 95/46/CE do Parlamento Europeu e do Conselho. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 10 set. 2020.

GB/T 35273-2017. Disponível em: http://pip.tc260.org.cn/assets/wz/2020-03-07/ef2dab88-cd9d-4748-814a-a3eca027beba.pdf. Acesso em: 10 set. 2020.

Lei de Proteção de Informações Pessoais e Documentos Eletrônicos. Disponível em: https://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html. Acesso em: 10 set. 2020.

Lei Federal de Proteção de Dados. Disponível em: https://www.gesetze-im-internet.de/bdsg_2018/. Acesso em: 10 set. 2020.

LGPD comentada. Disponível em: https://guialgpd.com.br/lgpd-comentada/. Acesso em: 10 set. 2020.

Princípios de privacidade australianos. Disponível em: https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-quick-reference/. Acesso em: 10 set. 2020.

Protección de los datos personales. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm. Acesso em: 10 set. 2020.

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679. Acesso em: 10 set. 2020.

Recebido em: 20/09/2020

Aprovado em: 03/11/2020