O APARENTE PARADOXO ENTRE A POLÍTICA DE OPEN JUSTICE E O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS

Paulo Eduardo Vieira de Oliveira
Fabrício Lima Silva

Resumo

A Lei Geral de Proteção de Dados inaugurou um novo normativo para o tratamento de dados realizado por pessoa natural ou por pessoa jurídica de direito público ou privado, no contexto de suas áreas de atuação, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Considerando-se o massivo tratamento de dados nos processos judiciais e princípio da publicidade dos atos processuais, surge a problemática sobre a necessidade de compatibilização da política de dados abertos (*open justice*) com a preservação da autodeterminação informativa e do direito fundamental à proteção de dados das partes envolvidas nos processos judiciais. É justamente sobre isso que se objetiva discorrer, a fim de apontar possíveis soluções que possam ser adotadas, de modo a orientar a implementação de medidas que garantam a privacidade dos titulares dos dados no âmbito dos processos judiciais.

Palavras-chave: Proteção de Dados, Dados Abertos e Autodeterminação Informativa.

Paulo Eduardo Vieira de Oliveira

Desembargador do TRT da 2ª Região (SP). Mestre e Doutor em Direito do Trabalho pela Faculdade de Direito da Universidade de São Paulo (FADUSP). Professor Doutor do Departamento de Direito do Trabalho da Faculdade de Direito da Universidade de São Paulo (FADUSP). Professor do Programa de Pós-Graduação em Direito da Faculdade de Direito do Sul de Minas (FDSM).

Fabrício Lima Silva

Juiz Titular da Vara do Trabalho de Teófilo Otoni (MG). Mestrando em Constitucionalismo e Democracia pela Faculdade de Direito do Sul de Minas (FDSM). Doutorando em Ciências Jurídicas Privatísticas pela Universidade do Minho (Portugal). Possui graduação em Direito pela Universidade de São Paulo, com habilitação em Direito de Empresa - Administração Empresarial e Tributária. Formação em Compliance Laboral pela Wolters Kluwer (Espanha). Formação como DPO pela Traininghouse (Portugal).

Abstract: The General Law of Data Protection has inaugurated a new regulation for the treatment of data performed by natural persons or public or private legal entities, in the context of their areas of activity, with the aim of protecting the fundamental rights of freedom and privacy and the free development of the personality of the natural person. Considering the massive treatment of data in judicial processes and the principle of the publicity of procedural acts, the problem arises about the need to make the policy of open data (open justice) compatible with the preservation of the informative self-determination and of the fundamental right to the protection of the data of the parties involved in the judicial processes. This is precisely what we intend to discuss, to point out possible solutions that may be adopted, to guide the implementation of measures that guarantee the privacy of data subjects in the scope of judicial proceedings.

Key words: Data Protection, Open Data, Informative Self-determination.

INTRODUÇÃO

Em 18 de setembro de 2020, com exceção das sanções administrativas[1], entrou em vigor a Lei n. 13.709/2018, que versa sobre a Lei Geral do Proteção de Dados (LGPD) em nosso país.

Por se tratar de uma lei geral, não foi o seu objetivo tratar de questões específicas como, por exemplo, os aspectos da proteção de dados na seara processual civil, trabalhista, penal ou militar. E, em razão disso, diversos aspectos ficaram pendentes de regulamentação e ainda nos trazem preocupações práticas sobre a compatibilização entre questões específicas e o regramento geral estabelecido.

A referida legislação disciplinou o tratamento de dados realizado por pessoa natural ou por pessoa jurídica de direito público ou privado, no contexto de suas áreas de atuação, com o objetivo de proteger os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A matéria sobre a proteção de dados pessoais em nosso país passou a ter como

1 As sanções administrativas passaram a ser exigíveis a partir de 1º agosto de 2021.

fundamentos: o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Por sua vez, em 10 de fevereiro de 2022, foi publicada a Emenda Constitucional n. 115/2022, que consagrou o direito fundamental à proteção dos dados pessoais, inclusive nos meios digitais (art. 5º, LXXIX, da CR).

Destacamos que, mesmo antes da alteração constitucional, existia o entendimento de que o referido direito já estava implicitamente positivado em nosso país, conforme fundamentação apresentada pelo STF, em decisão monocrática proferida pela Ministra Rosa Weber, na liminar proferida na ADI 6.387 MC-Ref/DF, em 06 de maio de 2020, que foi referenda pelo plenário da corte em 07 de maio de 2020.

Por outro lado, nosso texto constitucional sempre consagrou o princípio da publicidade processual, tendo como exceção a atribuição de sigilo aos julgamentos dos tribunais (art. 5º, LX e art. 93, IX, CR).

Tal previsão tem como fundamento a possibilidade de controle democrático sobre dos atos judiciais e a transparência no trato da coisa pública.

E, diante dos avanços tecnológicos ocorridos no Poder Judiciário Brasileiro, nas últimas décadas, surgiu o conceito de *open justice* (ou política de dados abertos), que ratifica a ideia de que os processos judiciais devem ser conduzidos com transparência e acesso público.

A partir do desenvolvimento de mecanismos de inteligência artificial, os dados judiciais passaram a ser utilizados para a identificação de diversas informações importantes que, a depender do contexto de uso, irão permitir a identificação de padrões estatísticos (jurimetria) ou a análise preditiva de julgados. Tal prática decorre de uma técnica desenvolvida a partir da década de 80, conhecida como mineração de dados (garimpagem, *profiling* ou *dataminig*), que consiste essencialmente em extrair informação de gigantescas bases de dados da maneira mais automatizada possível.[2]

2 AMO, Sandra de. Técnicas de Mineração de Dados. Disponível em: https://www.researchgate.net/profile/Sandra-Amo/publication/260300816_Tecnicas_de_Mineracao_de_Dados/

Nas últimas décadas, muito tem-se falado que os dados seriam o novo petróleo. Todavia, tal afirmação pode não ter a abrangência suficiente, uma vez que leva em consideração apenas o aspecto econômico do uso dos dados, como ativo financeiro. A depender do contexto, o uso dos dados pode gerar riscos às liberdades civis e aos direitos fundamentais, motivo pelo qual Sílvio Meira, apresentou o seguinte contraponto:

> DADOS não são o 'novo PETRÓLEO'. Comparando com fontes de energia, DADOS seriam o novo URÂNIO. Têm que ser REFINADOS para separar o que se quer do que não serve, têm que atingir MASSA CRÍTICA para gerar energia [VALOR!] e o DESCARTE é um perigo, para o negócio e o ecossistema.[3]

Conforme a orientação n.º 2016/679 do Grupo de Trabalho do Artigo 29 (GT-29), órgão consultivo criado com base na Diretiva n. 95/46/CE:

> A disponibilidade generalizada de dados pessoais na Internet e a partir de dispositivos da Internet das Coisas (IdC), bem como a capacidade para encontrar correlações e criar ligações, podem tornar possível determinar, analisar e prever aspetos que digam respeito à personalidade ou ao comportamento, aos interesses e aos hábitos de uma pessoa.[4]

Assim, o uso deliberado de tais ferramentas pode, em certos casos, implicar em violações a direitos e garantias fundamentais, com a adoção, por vezes, de práticas discriminatórias.

Nesse contexto, embora sejam inegáveis os benefícios que o uso da Inteligência Artificial, como, por exemplo, o aumento de eficiência e a economias de recursos, é importante que sejam estabelecidos e observados limites éticos e constitucionais.

Assim, importante o alerta feito pelo Grupo do Trabalho do Artigo 29 GT-29):

> A definição de perfis é suscetível de perpetuar os estereótipos existentes e a

links/54230bd80cf290c9e3ae25e3/Tecnicas-de-Mineracao-de-Dados.pdf. Acesso em: 09 de fev. 2023.

3 MEIRA, Sílvio. DADOS não são o 'novo PETRÓLEO'. Comparando com fontes de energia, DADOS seriam o novo URÂNIO. [...] Recife, 08 de jan. 2020. Twitter: @srlm. Disponível em: https://twitter.com/srlm/status/1214986628336250880. Acesso em: 09 de fev. 2023.

4 GT-29. Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679, de 03 de outubro de 2017. Disponível: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 15 de dez. de 2022.

> segregação social. Pode igualmente amarrar as pessoas a uma categoria específica e limitá-las às respetivas preferências sugeridas, pondo assim em causa a sua liberdade para escolher, por exemplo, determinados produtos ou serviços, tais como livros, música ou fluxos de notícias. Em certos casos, a definição de perfis é suscetível de resultar em previsões imprecisas. Noutros casos, poderá dar origem a uma negação de serviços e bens e a uma discriminação injustificada[5].

Na era da Big data, segundo Teresa Coelho Moreira[6], faz-se referência ao denominado *"trabalhador-transparente"* ou *"trabalhador de vidro"*, na medida em que a automatização da captura de dados do empregado pode, em muitos casos, incidir sobre aspectos que fazem parte de sua privacidade e que, portanto, deveriam ser protegidos.

Tais considerações possuem origem histórica fundada nas práticas adotadas pela polícia secreta do partido nazista alemão (Gestapo), que pretendia transformar os homens no *Gläserner Mensch* (homem de vidro), transparente e sem segredos, atuando como importante ferramenta para o exercício totalitarismo, com perseguições e injustas punições de grupos minoritários.

Apesar de a LGPD possuir como base legal para o tratamento de dados pessoais e de dados sensíveis o exercício regular de direitos em processo judicial (artigos 7º, VI e 11º, II, d, respectivamente), a exploração de tais dados fora do âmbito processual pode violar a privacidade e a intimidade das pessoas e atingir diversos aspectos de sua personalidade.

Nesse contexto, surge a problemática que iremos tratar no presente artigo: - Como compatibilizar a política de dados abertos adotada pelo Poder Judiciário brasileiro com o direito fundamental à proteção de dados e com a autodeterminação informativa dos jurisdicionados?

Nas linhas seguintes, iremos versar sobre a experiência europeia e, na sequência, trataremos da regulamentação dada pelo nosso Conselho Nacional de Justiça (CNJ), para, posteriormente, apresentarmos os possíveis problemas decorrentes da ausência de tratamento legislativo específico sobre matéria.

A PRECEDENTE DISCUSSÃO EUROPEIA

5 GT-29. *Ibidem.*

6 MOREIRA, Teresa Coelho Alexandra. A privacidade dos trabalhadores e a utilização de redes sociais online: algumas questões, in **Estudos de Direito do Trabalho.** v. 2. Coimbra: Almedina, 2016.

Como a LGPD brasileira teve forte influência da legislação europeia, importante o estudo preliminar sobre a regulamentação da questão dada pelo *General Data Protection Regulation* (GDPR) ao tratamento de dados feitos pelo Poder Judiciário no ambiente da União Europeia.

Em seu considerando n. 20, o GDPR destacou que sua regulamentação também é aplicável às atividades dos Tribunais, mas afastou a competência das autoridades de controle sobre o tratamento de dados pessoais feito pelos tribunais no exercício da sua função jurisdicional, objetivando assegurar a independência do Judiciário no exercício da sua função jurisdicional, nomeadamente a tomada de decisões.

Além disso, a alínea "a" do item 1 do art. 37 do GDPR dispensa a designação de encarregado de proteção de dados nos casos em que o tratamento for feito pelos tribunais no exercício de suas atividades jurisdicionais.

O item 3 do art. 55 do GDPR ratifica que as autoridades de controle não têm competência para fiscalização das operações de tratamento efetuadas pelos tribunais no exercício da sua função jurisdicional.

Com relação à mineração dos dados, o GDPR define como *profiling*:

> Qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações (art. 4º, item 4).

Assim, a definição de perfis possui três elementos: 1) tratamento automatizado; 2) deve incidir sobre dados pessoais; e 3) o seu objetivo deve ser avaliar os aspetos pessoais de uma pessoa singular[7].

Nos moldes do considerando 71 do GDPR, a definição de perfis pode levar em consideração:

> Aspetos pessoais relativos a uma pessoa singular, em especial a análise e previsão de aspetos relacionados com o desempenho profissional, a situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento,

7 GT-29. Ibidem.

> localização ou deslocações do titular dos dados, quando produza efeitos jurídicos que lhe digam respeito ou a afetem significativamente de forma similar.

Assim, a adoção de ferramentas de *profiling* pode fundamentar decisões com base em inferências e predições que consideram dados estatísticos/presunções, com a realização de algum juízo de valor, preferência ou critério pré-estabelecido.

Por sua vez, em se tratando de ordenamentos jurídicos nacionais, na França, em 23 de março de 2019, foi promulgada a Lei 2019-222, estabelecendo 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".[8]

E, no caso de infração à referida legislação, é prevista uma penalidade de até 5 (cinco) anos de reclusão.

A ideia defendida na França era a de coibir o uso de inteligência artificial para a coleta massiva de dados processuais, impedindo o uso de ferramentas de jurimetria ou de possível análise preditiva de julgados.

Em Portugal, o art. 206 da Constituição da República prevê, de forma semelhante ao Brasil, que as audiências dos tribunais serão públicas, salvo quando o próprio tribunal decidir o contrário, em decisão fundamentada, para salvaguarda da dignidade das pessoas e da moral pública ou para garantir o seu normal funcionamento.

O art. 164.º, n.º 3, do Código de Processo Civil de Portugal, estabelece que: "O acesso à informação do processo também pode ser limitado, em respeito pelo regime legal de proteção e tratamento de dados pessoais, quando, estando em causa dados pessoais constantes do processo, os mesmos não sejam pertinentes para a justa composição do litígio".

A lei n.º 32/2009, estabelece o regime jurídico aplicável ao tratamento de dados referentes ao sistema judicial em Portugal, sendo que, na base de dados das pesquisas jurisprudenciais, é possível a identificação do nome dos julgadores e, com relação às partes, se elas forem pessoas físicas, são apontadas apenas as suas iniciais, preservando-se a sua privacidade.[9]

8 FRANÇA. Lei nº 2019-222, de 23 de março de 2019. Disponível em: https://www.legifrance.gouv.fr/eli/loi/2019/3/23/2019-222/jo/article_33. Acesso em: 30 de nov. 2022.

9 O maior banco de dados de jurisprudência portuguesa é organizado pelo Supremo Tribunal de Justiça, encontrando-se disponível em: www.dgsi.pt/jstj.nsf/desc?OpenPage.

A ATUAÇÃO DO CONSELHO NACIONAL DE JUSTIÇA

O Conselho Nacional de Justiça (CNJ) foi criado pela Emenda Constitucional n. 45/2004 com o objetivo de efetuar o controle da atuação administrativa e financeira do Poder Judiciário e do cumprimento dos deveres funcionais dos juízes, cabendo-lhe, além de outras atribuições que lhe forem conferidas pelo Estatuto da Magistratura, desempenhar as atribuições previstas no art. 103-B da CR.

Em sua resolução n. 121, de 05 de outubro de 2021, o CNJ estabelecia que a consulta aos dados básicos dos processos judiciais deveria disponibilizada na rede mundial de computadores (internet), assegurado o direito de acesso a informações processuais a toda e qualquer pessoa, independentemente de prévio cadastramento ou de demonstração de interesse, ressalvados os casos de sigilo ou segredo de justiça (art. 1º).

Os dados de livre acesso seriam os seguintes: I – número, classe e assuntos do processo; II – nome das partes e de seus advogados; III – movimentação processual; e, IV – inteiro teor das decisões, sentenças, votos e acórdãos (art. 2º).

O acesso ao inteiro teor do processo deveria ser assegurado ao advogado cadastrado e habilitado nos autos, as partes cadastradas e o membro do Ministério Público (art. 3º).

E, posteriormente, em razão da promulgação da Lei n. 13.709/2018, que instituiu a Lei Geral de Proteção de Dados em nosso país, em 26 de abril de 2019, o CNJ, pela Portaria n. 63, instituiu um grupo de trabalho para elaborar estudos e propostas sobre a política de acesso às bases de dados dos processos judiciais dos Tribunais brasileiros, e especialmente o uso de tais informações para fins comerciais (art. 1º).[10]

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

10 CONSELHO NACIONAL DE JUSTIÇA (Brasil). Portaria n. 63, de 26 de abril de 2019. Disponível em: https://atos.cnj.jus.br/files/compilado043105202008065f2b8789824e1.pdf. Acesso em: 30 de nov. 2022.

e tratamento de dados de processos perante o Poder Judiciário.[11]

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

No referido relatório, foram apresentadas as seguintes recomendações:

> 1. **Dar continuidade à política de dados abertos** para o Poder Judiciário, com expansão da digitalização e disponibilização ao público dos pronunciamentos judiciais e autos dos processos, como forma de propiciar o controle democrático das instituições e servidores que compõe o sistema judiciário e de estímulo ao mercado digital;
> 2. **Aperfeiçoar o sistema de disponibilização de dados** por meio do desenvolvimento de projeto próprio que propicie a **interoperabilidade** entre as diferentes plataformas digitais de tramitação de processos e uniformize a forma de identificação dos processos, formato de disponibilização (*machinereadable format*), bem como os metadados relevantes de modo a facilitar buscas e criar as bases para o desenvolvimento de ferramentas inteligentes que permitam acessar, analisar e comparar decisões judiciais;
> 3. **Estimular a adoção de políticas de cache** pelas organizações que usam dados judiciais, como forma de reduzir a demanda de acesso aos servidores;
> 4. **Avaliar a adoção de uma API** (*application programming interface*) para acesso a dados judiciais, que proporcionará conveniência às organizações que realizam processamento automatizado de dados e permitirá aos tribunais controlar o formato do acesso aos dados e a qualidade da informação fornecida ao público;
> 5. **Avaliar** a realização de **projeto sobre anonimização de dados pessoais** em pronunciamento judiciais e em documentos disponibilizados ao público, para conciliar o amplo acesso aos dados processuais com a proteção de dados pessoais;
> 6. **Evitar a introdução de restrições ao acesso a documentos** presentes nos autos do processo que possam limitar o controle democrático das instituições que compõem o sistema judicial, como a ocultação de nomes de magistrados e servidores que participam da elaboração dos pronunciamentos judiciais;
> 7. Empregar **mecanismos que facilitem às partes a requisição de confidencialidade** de documentos de natureza sigilosa; e
> 8. **Difundir conhecimento** a respeito das exigências postas pela Lei Geral de Proteção de Dados para o acesso a dados judiciais, bem como dos requisitos de segurança da informação a serem observados, em especial no que diz respeito a **dados disponibilizados para o público[12]**.

Diante das conclusões apresentadas, verifica-se que o mencionado trabalho

11 LAWGORITHM. What is Lawgorithm? Disponível em: https://lawgorithm.com.br/en/about-us. Acesso em: 10 de dez. 2022.

12 LAWGORITHM. Acesso a Dados de Processos Judiciais no Brasil. Disponível em: https://lawgorithm.com.br/acesso-a-dados-de-processos-judiciais-no-brasil. Acesso em: 10 de nov. 2022.

procurou estimular a conciliação entre a proteção de dados pessoais, nas esferas pública e privada, com a tradição de abertura de dados de processos judiciais, possibilitando-se o controle democrático do sistema judiciário e o estímulo ao mercado digital, formado por *lawtechs* ou *legaltechs,* que oferecem serviços aos escritórios de advocacia, empresas ou instituições de ensino e pesquisa, tais como a identificação de padrões estatísticos ou de categorias comuns ao processos.

Para ampliação do acesso aos dados processuais, procurou-se estimular a adoção de modelos que permitam a interoperabilidade entre os diferentes sistemas processuais, em formato legível por máquina, com a facilitação de buscas e criação de bases de dados, a utilização de políticas de cache e adoção de uma API, que facilitaria o processamento automatizado dos dados.

Por outro lado, para preservação dos aspectos privados das partes envolvidas do processo, indicou-se a necessidade de realização de projeto sobre anonimização de dados pessoais existentes nos processos, com a adoção de mecanismos que facilitem a solicitação de confidencialidade em documentos sigilosos, a difusão das exigências impostas pela LGPD e a observância de requisitos de preservação da segurança da informação.

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

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

Houve a previsão de que os Tribunais poderiam avaliar a conveniência e oportunidade de cobrança pelo acesso massificado a dados, sendo que o valor da cobrança seria destinado a suportar os custos de implantação e manutenção do

sistema, devendo sua fixação ser efetuada na proporção do volume de dados utilizados (art. 3º).

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

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

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

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

A PREMENTE NECESSIDADE DE REGULAMENTAÇÃO DA APLICAÇÃO DA ANONIMIZAÇÃO DOS DADOS DAS PARTES E TESTEMUNHAS NOS PROCESSOS JUDICIAIS

Conforme sugerido no citado relatório elaborado pela Lawgorithm, o CNJ, ao regulamentar a questão, deveria avaliar a possibilidade de realização de projeto sobre anonimização de dados pessoais em pronunciamento judiciais e em documentos disponibilizados ao público, para conciliar o amplo acesso às informações processuais com a proteção de dados pessoais.

Segundo o disposto no inciso XI do art. 5º da LGPD, a anonimização seria a

"utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo". Por sua vez, nos moldes do inciso III do art. 5º da LGPD, dado anonimizado seria "dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento".

E, conforme o art. 12, caput, da LGPD, os dados anonimizados não serão considerados dados pessoais, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

O Grupo de Trabalho do Artigo 29º (GT29), criado pela Diretiva n. 95/46 da União Europeia, elaborou um parecer sobre técnicas de anonimização que reconhece a importância da anonimização de dados pessoais, em particular, como estratégia para colheita dos benefícios dos dados abertos para as pessoas e a sociedade em geral, reduzindo, simultaneamente, os riscos para as pessoas em causa.[13]

No âmbito da Justiça do Trabalho, diante da indevida exposição dos trabalhadores, sempre foi estabelecida restrição à consulta pública dos processos pelo nome das partes.

A questão, inclusive, foi objeto de análise pelo Órgão Especial do Tribunal Regional do Trabalho da 4ª Região (Rio Grande do Sul), que, ao interpretar as disposições da Resolução n. 121/2021 do CNJ, decidiu pela manutenção da restrição da pesquisa com base no nome das partes integrantes dos processos trabalhistas.

Na referida decisão foi ressaltada a preocupação de preservação da privacidade e intimidade do trabalhador, que integram o seu direito à personalidade, com o destaque para o fato de que, a depender do contexto do uso das informações obtidas, poderiam ser criados entraves de acesso ao mercado do trabalho e provocados constrangimentos ao trabalhador em razão do exercício do direito de ação.[14]

Sobre a necessidade de se repensar o modelo adotado atualmente, a título

13 GT-29. Parecer n. 05/2014, de 10 de abril de 2014. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_pt.pdf. Acesso em: 10 de dez. 2022.

14 TRF 4ª REGIÃO (Brasil). Acórdão n. 0000283-02.2014.5.04.0000 RECADM, de 21 de março de 2014. Disponível em: https://www.conjur.com.br/dl/orgao-especial-trt-derruba-pedido.pdf. Acesso em: 10 de dez. 2022.

exemplificativo, podemos indicar trechos de decisão disponibilizada no sítio eletrônico: www.jusbrasil.com.br, na qual são expostas informações privadas que permitem a identificação das partes envolvidas no processo e de testemunhas, em um contexto extremamente invasivo:

> "X" foi ouvido como informante, por ordem do juízo, e afirmou que teve um relacionamento passageiro com a reclamante, com seu consentimento.
> Ao final da audiência, "X" apresentou uma fotografia impressa com diversas imagens pequenas. Entre as imagens, há fotos que, supostamente, seriam da reclamante e de seus familiares, e outras de nudez (apenas partes do corpo, sem possibilidade de identificação). Ao exibir a fotografia, X declarou que a autora havia lhe (sic) enviado a maioria das imagens por WhatsApp e Skype. Afirmou que apagou as imagens de seu celular e que a reclamante lhe entregou a fotografia revelada em mãos. (...)
> Como ressaltado na origem, as alegações da autora foram comprovadas por meio de imagens de mensagens trocadas pelo aplicativo Skype, utilizado pela reclamante e por "X" como ferramenta de trabalho.
> O teor das mensagens não deixa dúvidas de que "X" utilizava o aplicativo para assediar a autora, importunando-a com mensagens inconvenientes, tais como, "Você está uma delícia!"; "Está muito mais linda"; "tempos que não te digo isso mais hoje você está diferente está mais linda!"; "quando a pessoal sabe que e linda nem responde um elogio!"; "princesa! se você quiser poso (sic) te fazer uma massagem!".[15]

Para fins do presente artigo, o nome da testemunha foi substituído por "X", mas, se acessado o inteiro teor do voto disponibilizado no referido portal, teríamos acesso ao nome completo da reclamante, da testemunha, da empresa e, além disso, da informação de que a autora era casada.

A referida situação fática permite a reflexão sobre a efetiva necessidade de indicação do nome dos autores e das testemunhas nas decisões tornadas públicas pelo Poder Judiciário. Em outras palavras: - para o controle democrático dos atos judiciais e análise dos indicativos jurisprudenciais seria necessária a publicização do nome das partes envolvidas no processo?

Sobre o tratamento de dados pelo Poder Público, já se manifestou nossa Autoridade Nacional de Proteção de Dados (ANPD):

15 TRT 3ª REGIÃO (Brasil), ROPS 0010354-57.2020.5.03.0040, de 11 de nov. 2020. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/trt-3/1125037293/inteiro-teor-1125037335. Acesso em: 10 de jan. 2023.

> 84. No setor público, o processo de adequação às disposições da LGPD tem suscitado muitas dúvidas a respeito dos parâmetros a serem observados para a disponibilização pública de informações pessoais. De forma geral, a análise dessas situações envolve uma ponderação entre direitos: de um lado, o direito à privacidade e o direito à proteção de dados pessoais e, de outro, o direito de todos os indivíduos à informação sobre as atividades do Poder Público. Este último se traduz, por exemplo, na divulgação, com base no interesse público, de informações relativas à execução de políticas públicas e ao exercício de competências legais pelos órgãos e entes públicos que permitam aos cidadãos o exercício do controle social sobre as atividades do Poder Público. Frequentemente, todavia, para atender ao princípio da publicidade, o Estado é obrigado a divulgar dados pessoais.
> 85. Enquanto o primeiro conjunto de direitos demanda uma posição de cautela e de análise de riscos a respeito da divulgação de informações pessoais, o segundo espelha a determinação legal de que a publicidade é a regra, admitindo-se o sigilo apenas em hipóteses excepcionais, nos termos da
> Lei de Acesso à Informação (Lei nº 12.527, de 17 de novembro de 2011 – LAI).
> 86. Não obstante, o tratamento de dados pessoais pelo Poder Público, incluindo a divulgação pública de dados pessoais, deve ser realizado em conformidade com as disposições da LGPD. Mais especificamente, devem ser observadas as normas que garantem a proteção integral dos dados pessoais, a autodeterminação informativa e o respeito à privacidade dos titulares durante todo o ciclo do tratamento.
> 87. Desde a realização da coleta até o fim da atividade realizada com os dados pessoais, conforme o caso, entidades e órgãos públicos devem, pelo menos, observar os princípios previstos na lei, verificar a base legal aplicável ao tratamento, garantir os direitos dos titulares e adotar medidas de prevenção e segurança, a fim de evitar a ocorrência de incidentes.
> 88. Nesse contexto, o cumprimento da LGPD demanda de entidades e órgãos públicos uma análise mais ampla, que não se limita à atribuição de sigilo ou de publicidade a determinados dados pessoais – este nem mesmo é o escopo da LGPD. Em termos práticos, considerando o reforço protetivo trazido pela LGPD ao titular de dados, é necessário realizar uma avaliação sobre os riscos e os impactos para os titulares dos dados pessoais bem como sobre as medidas mais adequadas para mitigar possíveis danos decorrentes do tratamento de dados pessoais.[16]

É importante que se diga que, diante da ausência de disposição legal específica ou de regulamentação do CNJ, no contexto legislativo atual, são formulados diversos pedidos, para que os processos tramitem em segredo de justiça ou para que os dados pessoais sejam anonimizados, sob o fundamento de um possível prejuízo em

16 ANPD (Brasil). Guia Orientativo: Tratamento de Dados Pessoais pelo Poder Público, versão 1.0, jan. 2022, págs. 20-21. Disponível em: https://www.gov.br/anpd/pt-br/documentos-epublicacoes/guia_tratamento_de_dados_pessoais_pelo_poder_publico___defeso_eleitoral.pdf. Acesso em: 08 de dez. 2022.

futuras contratações por meio das "listas sujas de trabalhadores", havendo decisões divergentes sobre tal questão. Algumas acolhem o pedido de supressão dos nomes das partes, com base na LGPD (Processo: 1000902-06.2019.5.02.0707 e outras), enquanto outras entendem que a proteção conferida pelas regras vigentes já seria suficiente, indeferindo tal pleito (Processo: 1001089-83.2020.5.02.0317 e outros).[17]

Assim, para garantia da privacidade das partes e testemunhas, com a preservação da autodeterminação informativa e garantia do direito fundamental à proteção de dados, faz-se necessária a adoção de meios para a anonimização dos registros tornados públicos pela política de *open justice* adotada pelo CNJ.

Nem se diga que a adoção de tal medida inviabilizaria a atuação das *lawtechs,* pois, conforme destacado no supracitado relatório da Lawgorithm, a atuação das referidas empresas concentram-se mais nos pronunciamentos judiciais, nas petições e, em menor medida nos documentos pessoais das partes, sem a exploração dos aspectos pessoais das partes. Tal constatação demonstra que eventual medida de anonimização dos dados identificadores de pessoas físicas envolvidas nos processos teria pouco impacto nas atividades de tecnologia aplicada aos dados judiciais, sendo fundamental para a proteção da privacidade dos envolvidos.[18]

Destacamos que todo o tratamento de dados deve observar, dentre outros, o princípio da necessidade, segundo o qual deve existir a "limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados" (art. 6º, III, da LGPD).

Nesse contexto, considerando-se a divulgação dos dados processuais pelo Poder Judiciário como uma operação de tratamento, para o cumprimento da finalidade de publicidade processual, entendemos seria desnecessária a divulgação do nome das partes envolvidas.

CONSIDERAÇÕES FINAIS

A partir da vigência da LGPD e da promulgação da Emenda Constitucional n. 115/2022, que consagrou o direito fundamental à proteção dos dados pessoais, inclusive

17 ALMEIDA, Isaac Nogueira de; BARZOTTO, Luciene Cardoso. Lei Geral de Proteção de Dados versus Lei de Acesso a Informações: aparente conflito entre normas. No prelo.

18 Ibidem.

nos meios digitais (art. 5º, LXXIX, da CR), inaugurou-se um novo marco de proteção aos direitos da personalidade em nosso país.

E, diante desse novo cenário, no presente artigo procuramos analisar o aparente conflito existente entre o princípio da publicidade dos atos processuais e o direito fundamental à proteção de dados, com a demonstração de que seria possível a compatibilização entre os referidos direitos fundamentais.

As medidas de anonimização dos dados pessoais tornados públicos pelo Poder Judiciário demonstram-se ser suficientes para o cumprimento da missão de valorização do controle democrático das instituições e respeito à proteção do direito fundamental à proteção de dados (art. 5º, LXXIX, da CR).

Assim, para que sejam atendidas as exigências de publicidade e de preservação da privacidade nos envolvidos nos processos judiciais, com o respeito ao princípio da necessidade, importante adoção de medidas de anonimização dos dados pessoais sempre que tal procedimento não comprometa a finalidade do tratamento.

BIBLIOGRAFIA

ALMEIDA, Isaac Nogueira de; BARZOTTO, Luciene Cardoso. **Lei Geral de Proteção de Dados versus Lei de Acesso a Informações:** aparente conflito entre normas. No prelo.

AMO, Sandra de. **Técnicas de Mineração de Dados.** Disponível em: https://www.researchgate.net/profile/Sandra-Amo/publication/260300816_Tecnicas_de_Mineracao_de_Dados/links/54230bd80cf290c9e3ae25e3/Tecnicas-de-Mineracao-de-Dados.pdf. Acesso em: 09 de fev. 2023.

ANPD (Brasil). **Guia Orientativo:** Tratamento de Dados Pessoais pelo Poder Público, versão 1.0, jan. 2022, págs. 20-21. Disponível em: https://www.gov.br/anpd/pt-br/documentos-epublicacoes/guia_tratamento_de_dados_pessoais_pelo_poder_publico___defeso_eleitoral.pdf. Acesso em: 08 de dez. 2022.

CONSELHO NACIONAL DE JUSTIÇA (Brasil). **Portaria n. 63, de 26 de abril de 2019.** Disponível em: https://atos.cnj.jus.br/files/compilado043105202008065f2b8789824e1.pdf. Acesso em: 30 de nov. 2022.

FRANÇA. **Lei nº 2019-222, de 23 de março de 2019.** Disponível em: https://www.legifrance.gouv.fr/eli/loi/2019/3/23/2019-222/jo/article_33. Acesso em: 30 de nov. 2022.

GT-29. **Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679, de 03 de outubro de 2017.** Disponível: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 15 de dez. de 2022.

_____. **Parecer n. 05/2014, de 10 de abril de 2014.** Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_pt.pdf. Acesso em: 10 de dez. 2022.

LAWGORITHM. **Acesso a Dados de Processos Judiciais no Brasil.** Disponível em: https://lawgorithm.com.br/acesso-a-dados-de-processos-judiciais-no-brasil. Acesso em 10 de nov. 2022.

_____. ***What is Lawgorithm?*** Disponível em: https://lawgorithm.com.br/en/about-us. Acesso em: 10 de dez. 2022.

MEIRA, Sílvio. **DADOS não são o 'novo PETRÓLEO'. Comparando com fontes de energia, DADOS seriam o novo URÂNIO.** [...] Recife, 08 de jan. 2020. Twitter: @srlm. Disponível em: https://twitter.com/srlm/status/1214986628336250880. Acesso em: 09 de fev. 2023.

MOREIRA, Teresa Coelho Alexandra. A privacidade dos trabalhadores e a utilização de redes sociais online: algumas questões, in **Estudos de Direito do Trabalho.** v. 2. Coimbra: Almedina, 2016.

TRF 4ª REGIÃO (Brasil). **Acórdão n. 0000283-02.2014.5.04.0000** RECADM, de 21 de março de 2014. Disponível em: https://www.conjur.com.br/dl/orgao-especial-trt-derruba-pedido.pdf. Acesso em: 10 de dez. 2022.

TRT 3ª REGIÃO (Brasil), **ROPS 0010354-57.2020.5.03.0040,** de 11 de nov. 2020. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/trt-3/1125037293/inteiro-teor-1125037335. Acesso em: 10 de jan. 2023.