ARTIGO RECEBIDO EM 26/09/2025 E APROVADO EM 13/06/2025 DOI: HTTPS://DOI.ORG/10.56267/RDTPS.V11I21.18463

A PROTEÇÃO DE DADOS E AS RELAÇÕES LABORAIS NO BRASIL

José Antonio Siqueira Pontes[1]
Daniel Oliveira da Silva[2]

Resumo: O presente trabalho tem como tema principal os impactos da proteção de dados pessoais na relação laboral, avaliando os marcos regulatórios jurídicos para garantia desse importante direito fundamental à privacidade e delineando alguns limites na relação contratual laboral, especialmente os relacionados à proteção de dados dos empregados. O estudo pretende partir da importância da proteção dos dados pessoais na atualidade e de sua regulamentação nacional e estrangeira e revelar como se dá sua proteção na relação laboral no mundo globalizado. O objetivo principal é indicar parâmetros para deveres do empregador na coleta e processamento de dados pessoais de empregados, com olhar específico nos seus direi-

[1] Prof. pesquisador da graduação em direito e do mestrado acadêmico do Centro Universitário das Faculdades de Campinas - Brasil. (PPGD-FACAMP). Mestre e Doutor em direito pela Universidade de São Paulo (USP). Coordenador do grupo de pesquisas em compliance empresarial da Facamp - Editor-chefe da Revista DESC (desc.facamp.com.br). Prof. da graduação em direito da Faculdade de Direito de Sorocaba (FADI)/Brasil.
E-mail: jose.pontes@facamp.com.br, jspontes@gmail.com
Lattes: http://lattes.cnpq.br/3712312436960179
ORCID: https://orcid.org/0000-0003-4580-286X

[2] Estudante do mestrado acadêmico do Centro Universitário das Faculdades de Campinas, Brasil. Bacharel em direito pela Pontifícia Universidade Católica de Campinas. Especialista em Direito Empresarial pela Fundação Getútio Vargas (FGV), especialista em Direito Civil e Processo Civil pelas Faculdades Integradas de Campinas (Metrocamp), especialista em Direito Societário pela Escola Paulista de Direito (EPD) e especialista em Compliance pela IBMEC. Membro do grupo de pesquisas em compliance empresarial da Facamp.
E-mail: danielsilva1987@hotmail.com
Lattes: https://lattes.cnpq.br/5122957501464045
ORCID: https://orcid.org/0009-0006-2932-6073

tos de uso e compartilhamento desses dados. Por fim, apresenta-se a tese de vanguarda no tema: o possível conflito existente entre o legítimo interesse do empregador e o livre consentimento do empregado, levando à identificação da necessária avaliação de riscos do grau de interesse legítimo do empregador, o que representa uma contribuição do debate atual na área de regulação digital para a relação laboral. Se utiliza o método dedutivo, por meio de pesquisas bibliográficas na doutrina, legislação, revistas e sites, para se chegar à conclusão de que, pela força das inovações regulatórias e doutrinárias, procedimentos internos adotados pelo empregador em termos de avaliação de riscos e legítimo interesse devem levar a um salto na qualidade da relação laboral no que diz respeito à coleta e ao tratamento de informações pessoais dos empregados.

Palavras-chave: Proteção de Dados Pessoais; Relação laboral; LGPD; Legítimo interesse.

DATA PROTECTION AND LABOR RELATIONS IN BRAZIL

Abstract: This work primarily examines the impacts of personal data protection in labor relationships, evaluating legal regulatory frameworks to ensure this fundamental right to privacy and outlining some limits in the employment contractual affairs, especially concerning employee data protection. The study emphasizes the importance of personal data protection today and its national and international standards and its protection in the globalized social relations. The main objective is to indicate parameters for employer duties in collecting and processing employees' personal data, focusing on their rights to use and share this data. Finally, it presents a pioneering thesis on the topic: the potential conflict between the employer's legitimate interest and the employee's free consent, leading to the necessary risk assessment of the employer's degree of legitimate interest, contributing to the current debate in digital regulation with regard with labor law. The deductive method is used through bibliographic research in doctrine, legislation, scientific reviews, and websites, concluding that, due to regulatory and

doctrinal innovations, internal procedures adopted by the employer including risk assessment and legitimate interest should lead to a qualitative leap in the labor relations concerning to the collection and the processing of employees' personal information.

Keywords: Personal Data Protection; Labor law; GDPR; Legitimate interest.

Introdução

No atual estágio da globalização das relações sociais e econômicas, a rapidez, a impessoalidade e a eficiência das trocas mercantis são os aspectos predominantes, mediadas pelas informações em novo papel de destaque. Nunca, na história a ideia de que "informação é poder" foi tão evidente (CASTELLS, 1999), (BIONI, 2019, p.5)

O fenômeno da sociedade da informação se intensificou nos anos 2000 com o nascimento de infraestruturas tecnológicas de coleta, armazenamento e processamento de grandes quantidades de dados, que passou a ser nomeada como *Big Data*. No Ocidente, de seu berço no Vale do Silício nasceram *Google* (1998), *Wikipedia* (2001), *Youtube* (2005), *Facebook* e *Twitter* (2006), *iPhone* e *Android* (2007) etc., empresas e produtos que impulsionaram o *Big Data*, caracterizado por seu volume, com *terabytes* ou *petrabytes*; a alta velocidade dos bancos de dados, em tempo real; seu âmbito ampliado para captar informações de populações e sistemas inteiros; sua flexibilidade para adicionar funções, processar e expandir rapidamente. (TÉLLEZ CARVAJAL, 2020)

Em casos mais usuais nas relações sociais em redes digitais, o uso de *cookies*, *profiling* e *machine learning* **(i)** identifica, antecipadamente e qualitativamente, o real interesse das pessoas como

potenciais clientes, com base em dados estatísticos e parametrizados; **(ii)** conecta produtos semelhantes ao perfil do usuário para lhe ajudar na formação da ideia de compra, (**iii)** amplia a atuação geográfica de fornecedores com enorme vantagem competitiva e economia de recursos.

Por um longo período, essas novas interações sociais globalizadas permaneceram sem regulamentação específica por nações ou organismos internacionais, de modo que os dados pessoais foram utilizados de forma livre e inovadora por governos e grandes empresas sem autorização prévia de seus titulares, inclusive lucrando com eles via "monetização de dados". A regulação jurídica tornou-se imperativa, especialmente após a identificação de prejuízos a uma enorme parcela da sociedade com vazamentos de dados e outros problemas relacionados à segurança individual e coletiva.[3]

O passo mais recente de Estados e organismos internacionais para regulamentar essas tendências irrefreáveis foi a aprovação de leis de proteção dos dados pessoais e privacidade, dando novo rumo ao cenário anterior, de pouca ou nenhuma supervisão jurídica e grande descompasso entre os interesses dos titulares de dados pessoais e sua proteção, quando muito remediada por meio de ações civis individuais ou de direitos do consumidor (DONEDA, 2006.). Em resumo, enquanto os dados pessoais se tornavam um ativo valiosíssimo na economia global, sua proteção jurídica ganhou corpo em inúmeras nações e organismos internacionais.

[3] Apenas o escândalo *Cambridge Analytica* indicou que cidadãos foram prejudicados em sessenta e oito países, oitenta e sete milhões de usuários com possível influência nos resultados do "Brexit" das eleições de 2018 no Brasil, cf. NYT, 2018 e GAIATO, 2020.

Nesse contexto, observa-se que os dados pessoais[4] se tornaram o "novo petróleo" (PALMER, 2006), pois quem detém esse ativo pode convertê-lo com grande facilidade em negócios de diferentes formas e por diferentes meios. Os dados são transportáveis sem custos logísticos e sem qualquer limitação de fronteiras territoriais por estarem em formato virtual e são passíveis de "tratamento digital" (BRASIL, 2018) para gerar produtos derivados da sua "mineração", segundo terminologia atual (TAN; STEINBACH; KUMAR, 2016).

O presente estudo pretende analisar a proteção dos dados pessoais no direito brasileiro sob o prisma de uma das áreas mais afetadas nesse tema, que é a do direito laboral. É comum a situação de empregados que, no âmbito da relação laboral, revelam seus dados pessoais por diversas razões aos seus empregadores. Em muitas oportunidades, em razão da função, outros empregados possuem acesso aos dados pessoais de colegas. A partir dos marcos jurídicos regulatórios da proteção de dados em nível nacional e internacional, o presente estudo tem como objetivo primordial delinear parâmetros precisos para os deveres do empregador na coleta e processamento de dados pessoais de empregados, com enfoque particular nos direitos de uso e compartilhamento dessas informações.

Ademais, apresenta-se uma tese de vanguarda no campo: a identificação de um possível conflito entre o interesse legítimo do empregador e o consentimento livre e informado do empregado, o que exige uma avaliação rigorosa dos riscos associados ao grau de

[4] Segundo o artigo 5º, inciso I da Lei 13.709, de 14 de agosto de 2018, denominada "Lei Geral de Proteção de Dados - LGPD, dado pessoal é conceituado como "informação relacionada a pessoa natural identificada ou identificável". (BRASIL, 2018).

interesse legítimo do empregador. Esta análise representa uma contribuição significativa ao debate contemporâneo sobre regulação digital aplicada às relações laborais. A hipótese para a uma conclusão indica que inovações regulatórias e doutrinárias recentes somados aos procedimentos internos de avaliação de riscos e de interesse legítimo adotados pelos empregadores devem proporcionar um avanço substancial na qualidade das relações de trabalho, especialmente no que tange aos direitos dos empregados diante da coleta e do tratamento de seus dados pessoais.

A Proteção de Dados Pessoais

Relevância Econômica e Social

Para além de seu valor econômico, os dados pessoais têm enorme relevância social, política e científica, regionalmente e globalmente, uma vez que, por meio deles é possível: **(i)** identificar e mensurar quantitativamente comportamentos e características de grupos sociais, cidades, países, serviços etc., seus problemas e possíveis soluções; **(ii)** elaborar políticas públicas com assertividade, determinado o grupo e o local onde devem ser realizados para que os melhores resultados sejam obtidos; **(iii)** fomentar pesquisas acadêmicas com recortes específicos utilizando-se dados estatísticos; **(iv)** causar ou evitar segregação de pessoas ou grupos (FERNÁNDEZ; FERRER, 2016); (BIDERMAN *et al*., 2021).

Em meio à circulação de *big data* estão também os chamados dados pessoais sensíveis. Segundo o que define a Lei Geral de Proteção de Dados ("Lei 13.709, de 14 de agosto de 2018" - LGPD),

dados pessoais sensíveis são aqueles indicados no artigo 5º, inciso II como "dado pessoal sobre 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". (BRASIL, 2018).

Essa subespécie de dado pessoal tem enorme potencial para gerar discriminação e até mesmo violência verbal e física. Por exemplo, basta imaginar pessoas da comunidade LGBTQIA+, infelizmente, em determinados países ou **círculos sociais, precisam esconder** que pertencem a tal grupo para não sofrerem nenhum tipo de violência, física e verbal. Outras situações como informações sigilosas de filiação a sindicatos ou outras associações, infecções sexualmente transmissíveis ou doença que cause estigma, exercício de crença religiosa em países ou regiões sem plena liberdade de culto, se não forem protegidas, podem expor indivíduos e coletividades a riscos desmedidos e inaceitáveis. (FREITAS; PIMENTA, 2014), (CHIAVEGATTO FILHO, 2015); (RAUTENBERG; CARMO, 2019, p. 57).

Tudo isso nos leva a crer que a sociedade da informação, como se evidencia acima, trouxe novas preocupações aos direitos individuais, em específico quanto aos limites e a legitimidade para utilização dos dados pessoais nas diversas relações entre usuários e empresas de tecnologia, mas não só, em todas as relações privadas e com entidades públicas que envolvem coleta de informações. Se a face empreendedora da revolução telemática são os *big data,* a face ética, jurídica e regulatória é o direito de proteção de dados para tutela e a proteção das pessoas por trás dos *bytes*.

Regulamentação da Proteção de Dados.

Os parâmetros internacionais para a regulação jurídica da proteção de dados não são tão recentes. A **título de** exemplo tem-se **(i)** Organização das Nações Unidas, por meio da Resolução 71/199, adotada por sua Assembleia Geral em 2017, estabeleceu um conjunto de princípios para a proteção da privacidade, na sociedade de informação (UN, 2017) e a Organização Internacional do Trabalho (OIT), no mesmo sentido, criou um código de conduta específico para as relações laborais em 1997 (ILO, 1997); **(ii)** Conferência Internacional de Proteção de Dados e Privacidade (ICDPPC, 2018), que reúne autoridades de proteção de dados pessoais do mundo todo, com o fito de promover a colaboração e princípios globais de proteção de dados pessoais (IDCPPC, 2018); **(iii)** outros documentos "*soft*" de guia para países membros de organismos internacionais, como Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais (OCDE, 2003); **(iv)** documentos com força vinculativa, como o Acordo Schrems II, que estabelece regras para transferência de dados pessoais de titulares europeus para países localizados fora da Europa (CORBET; et al., 2020); **(v)** regulamentos da União Europeia, como a Convenção Europeia de 1981, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,* atualizada para "Convenção 108+" (COE, 2018), com uma regulação mais robusta a partir de 1995 dada pela diretiva *Data Protection Directive (95/46/EC)* (EUR-lex, 1995). **(vi)** legislações nacionais mais específicas e atuais de diversos países e da União Europeia sobre processamento e compartilhamento de dados nacional e internacionalmente. (NAIR; TYAGI, 2021)

Diversos organismos internacionais como, por exemplo, a *Eletronic Frontier Foundation (EFF, 2022)* e a *Privacy International* (PRIVACY INTERNATIONAL, s/d), produzem relatórios, índices orientações *soft* com o objetivo de avaliar o nível de proteção de dados dos mais diferentes países, atualizar o estado das tecnologias e suas regulamentações, trocar orientações entre empresas e governos.

Sobre as leis de proteção de dados pessoais mais modernas e impactantes, importa notar que a primeira a influenciar e inspirar o restante do mundo foi da União Europeia, que criou em 2016, a *General Data Protection Regulation* (GDPR) (EUR-Lex, 2016) para disciplinar a forma como as organizações localizadas na União Europeia ou fora dela devem tratar os dados pessoais de cidadãos europeus. (RUSTAD; KOENIG, 2019)

O Brasil, por sua vez, teve regulamentadas as hipóteses, formas, direitos dos titulares dos dados pessoais, deveres dos operadores, sanções aplicáveis a infrações, constituição da autoridade competente para fiscalizar os tratamentos de dados entre outras questões por força da LGPD. (BRASIL, 2018).

A LGPD foi inspirada na legislação europeia de proteção de dados (GDPR), razão pela qual adotou os mesmos princípios norteadores, o que facilita a aplicação de conceitos gerais, considerando que as duas legislações possuem como característica a transnacionalidade e estão tratando de fenômeno globalmente padronizado no atual estágio do capitalismo.

Mas apenas no direito brasileiro os dados pessoais foram elevados **à** categoria de direito fundamental (ARAUJO; NUNES JÚNIOR, 2007 p. 71- 72), sendo incorporados na Constituição Federal, precisamente no artigo 5º, inciso LXXIX, em razão da aprovação da

Emenda Constitucional nº 115, de 10 de fevereiro de 2022. (BRASIL "a", 2022). H**á quem sustente** que, além de se tratar de um direito fundamental, os dados pessoais integram a categoria dos direitos da personalidade. (BIONI, 2019, p.62)

Dessa forma, diante de regramento específico e do status alcançado de direito fundamental, a proteção dos dados pessoais deve acontecer em todos os momentos e em qualquer relação jurídica na qual as pessoas físicas forneçam, por qualquer meio, seus dados pessoais.

A máxima deve ser a transparência no seu uso, de modo que seu titular saiba quais e como seu dado será tratado antes da sua coleta, para qual finalidade será utilizado, por quanto tempo será armazenado e por quem, de modo que, caso queira, o titular dos dados pessoais possa utilizar dos direitos que a lei lhe confere, como, por exemplo, determinar a sua correção ou exclusão da base de dados do agente do tratamento de dados.

A lei brasileira não impede o "tratamento de dados pessoais" (BRASIL, 2018), apenas regula como tais dados devem ser manipulados e as precauções que devem ser adotadas para sua proteção ou para impedir que terceiros estranhos tenham acesso aos dados sigilosos e sensíveis. O objetivo da legislação é evitar abusos, como, por exemplo, a venda de banco de dados de clientes para ou por empresas de telemarketing, prática frequente em um passado não tão distante. Com base em escândalos recentes, o potencial destrutivo que a divulgação inadvertida de dados pessoais (sensíveis ou não) pode causar a seus titulares **é** imensurável, reforçando a necessidade de sua proteção. Casos de divulgação inadvertida de dados pessoais surgem cada vez mais no Brasil, a exemplo dos vazamentos ocorri-

dos pelo SERASA / BOA VISTA/ Receita Federal/ INSS, em que se estima que dados de 220 milhões pessoas foram revelados, contendo informações econômicas de seus titulares, vendidos no mercado paralelo pela bagatela de R$ 200,00 (duzentos reais). (MARCELINO, 2024) (G1, 2021).

Proteção de Dados na relação laboral

Essas características analisadas até aqui revelam uma lógica global na área de proteção de dados com especial atenção ao fenômeno do *Big Data,* que são dados massivos de terceiros sem qualquer relação contratual com os agentes de tratamento de dados, como é o caso das empresas de *Big Tech* ou entidades a elas equiparadas. Porém qualquer entidade ou organização, sendo pessoa jurídica de natureza pública ou privada, grande ou pequena, e até pessoas físicas ficam sujeita aos deveres específicos da LGPD e da rede de legislações internacionais com efeito extraterritorial. A questão que se deseja enfrentar na presente pesquisa é o que acontece quando os dados coletados e tratados são das pessoas *interna corporis,* ou seja, que trabalham ou se candidatam para trabalhar na pr**ópria organização ou entidade.** Aqui fica evidente uma intersecção entre as áreas de proteção de dados e direito do trabalho.

Nas relações laborais, a coleta e o tratamento de dados pessoais e sensíveis podem acontecer durante toda relação, primeiro na relação pré-contratual (tratativas), para estabelecer um primeiro contato e favorecer a possível contratação do candidato. Segundo, porque, para efetivar a contratação, as empresas necessitam cumprir obrigações legais junto a órgãos governamentais, prestar informa-

ções a autoridades, realizar seu tratamento devendo o empregador solicitar ao empregado seus dados pessoais, inclusive aqueles denominados pela lei como "dados pessoais sensíveis", oportunidade em que importa fundamentar sua necessidade entre as dez hipóteses para o tratamento de dados pessoais e as sete hipóteses legais que autorizam o tratamento de dados pessoais sensíveis segundo os artigos 7 e 11 da LGPD, respectivamente. (BRASIL, 2018)).

A LGPD não faz menção expressa à proteção de dados pessoais no contexto das relações de trabalho, diferentemente do GDPR europeu, que menciona o tema no seu artigo 88:

> Tratamento no contexto laboral
> 1. Os Estados-Membros podem estabelecer, no seu ordenamento jurídico ou em convenções coletivas, normas mais específicas para garantir a defesa dos direitos e liberdades no que respeita ao tratamento de dados pessoais dos trabalhadores no contexto laboral, nomeadamente para efeitos de recrutamento, execução do contrato de trabalho, incluindo o cumprimento das obrigações previstas no ordenamento jurídico ou em convenções coletivas, de gestão, planeamento e organização do trabalho, de igualdade e diversidade no local de trabalho, de saúde e segurança no trabalho, de proteção dos bens do empregador ou do cliente e para efeitos do exercício e gozo, individual ou coletivo, dos direitos e benefícios relacionados com o emprego, bem como para efeitos de cessação da relação de trabalho. (EUR, 2016)

Porém, por princípio, uma proteção de dados pessoais do empregado é fundamental para que essa relação cumpra as diretrizes gerais da LGPD brasileira em termos semelhantes à diretiva europeia. O empregador poderá solicitar ao empregado e, em algumas situações, este não lhe poderá negar informações sensíveis ou outras que podem gerar algum risco, razão pela qual o empregador terá o inequívoco dever de as proteger com o máximo de cuidado e diligên-

cia. Por exemplo, dados sobre orientação sexual e outros indicados no artigo 5º, inciso II da LGPD **são de coleta obrigatória nos exames médicos** admissionais e periódicos legalmente exigidos pelo art. 168 da CLT (BRASIL, 1943) e podem causar a sua segregação dentro da organização, perante os demais empregados, ou mesmo fora, na sociedade civil.

> Assim sendo, em termos concretos, afirma-se que os impactos trazidos pela LGPD para as relações de emprego perpassam pela obrigatoriedade de análise minuciosa dos trâmites internos de coleta e tratamento de dados por parte dos empregadores, no intuito de garantir a adequação de seu respectivo sistema interno à legislação vigente, uma vez que os ditames do dispositivo devem ser observados desde o processo seletivo para contratação do novo empregado, até após a dissolução do contrato de trabalho, imputando responsabilidade civil ao empregador desde o momento da captação dos dados.(FERREIRA; FALCÃO; BIZZOCCHI, 2022, p. 234)

Por esse motivo, o Código de Conduta da OIT deve ser observado sempre que possível quando determina que dados sensíveis do empregado, em regra, não devem ser solicitados pelo empregador, salvo em caso de necessidade justificada:

> 6.5 (1) Um empregador não deve coletar dados pessoais relativos a um trabalhador sobre: (a) vida sexual; (b) crenças políticas, religiosas ou outras; (c) condenações criminais. (2) Em circunstâncias excepcionais, um empregador pode coletar dados pessoais relativos aos itens mencionados em (1) acima, se os dados forem diretamente relevantes para uma decisão de emprego e em conformidade com a legislação nacional.
> 6.6. Os empregadores não devem coletar dados pessoais relativos à filiação do trabalhador a uma organização de trabalhadores ou às atividades sindicais do trabalhador, a menos que sejam obrigados ou permitidos por lei ou por um acordo coletivo.
> 6.7. Dados médicos pessoais não devem ser coletados, exceto em conformidade com a legislação nacional, a confidencialidade médica e os

> princípios gerais de saúde e segurança ocupacional, e somente conforme necessário: (a) para determinar se o trabalhador está apto para um emprego específico; (b) para cumprir os requisitos de saúde e segurança ocupacional; e (c) para determinar o direito a, e conceder, benefícios sociais. (ILO, 1997)

Fica evidente que, diante da importância dos dados pessoais e do seu fluxo nos sistemas internos da entidade empregadora, entram em foco os pilares da LGPD como consentimento, finalidade e legítimo interesse na específica relação laboral, que passam a ser analisados conforme a situação para se fazerem cumprir os deveres do empregador ou do empregado, que tem óbvias obrigações de proteção de dados alheios a que tenha acesso por força de sua atividade laboral.

Deveres do empregador.

O empregador, no âmbito da lei nacional de proteção de dados, é "pessoa natural ou pessoa jurídica de direito público ou privado" e tem o dever legal de zelar pelos dados pessoais que recebe de seus empregados. A não observância das inúmeras obrigações que a lei determina traz como consequência as sanções contidas no artigo 52 da LGPD, com multas que podem chegar a cinquenta milhões de reais. (BRASIL, 2018)

A aplicação das sanções administrativas trazidas pela LGPD é, em princípio, competência da Agência Nacional de Proteção de Dados (ANPD), porém essa não é a única modalidade de sanção prevista, ou seja, deve-se analisar se em qual âmbito, laboral, consumerista ou civil, o ilícito aconteceu. O Ministério Público do Trabalho (MPT), sendo o órgão responsável por fiscalizar as relações laborais, pode identificar situação de vazamento de dados de determinada

pessoa jurídica e solicitar sanções administrativas. Essa seria uma leitura do disposto no parágrafo §3º do artigo 42 da LGPD, sobre a possibilidade de ingresso de ações coletivas, para buscar reparação de danos causados pela coletividade (BRASIL, 20218)

Nesse sentido, o MPT, em fiscalização ou após denúncia, reconhecendo violações dos princípios de proteção de dados pessoais no âmbito da relações laborais ou em razão delas, poderia demandar sanções administrativas em tutela de direitos individuais homogêneos (DIDDIER JR; ZANETI JR. 2009, p. 76-77) por meio de Ação Civil Pública[5], buscando reparação dos danos e providências para que tal conduta seja corrigida. (DOS SANTOS; LIMA 2020).

Ainda no âmbito dos interesses e dissídios coletivos, discute-se a possibilidade de os sindicatos poderem estabelecer regras em matéria de proteção de dados de empregados sindicalizados. A crescente e recente flexibilização dos direitos e proteções do empregado no Brasil aponta para a tendência da primazia do negociado sobre o legislado, porém respeitável doutrina levanta objeções em termos da constitucionalização dos dados como face de direitos individuais inalienáveis por força de sua elevação a direito fundamental.

Na outra face do direito laboral brasileiro, estão os dissídios individuais. Na hipótese de um empregado sofrer a violação de seu

[5] Vide, por exemplo, Ação Civil Pública - 0730600-90.2020.8.07.0001 que o Ministério Público do Distrito Federal: (i) dados pessoais de brasileiros não fossem cedidos a qualquer título, já que foram tratados de forma irregular, (ii) que a ré fosse condenada a eliminar todos os dados tratados de forma irregular que possui em sua base de dados. Ainda que não seja no âmbito das relações laborais, a legitimidade para defesa dos dados pessoais dos empregados pelo Ministério Público Trabalho é a mesma, qual seja, a tutela de interesses individuais homogêneos, por força das Lei n. 7.347/85, que disciplina a Ação Civil Pública, e da Lei Geral de Proteção de Dados. (SOUZA, 2021).

direito relativo à proteção de dados pessoais, poderia buscar a indenização correspondente na justiça trabalhista, seja por perdas e danos ou danos morais, com fulcro, inclusive na Constituição Federal. (BRASIL, 2021)

Na justiça trabalhista, os juízes e tribunais já iniciaram a formação da jurisprudência em vários temas relativos à LGPD, dentre eles também dissídios individuais que tocam especificamente os direitos à proteção de dados do trabalhador como direito fundamental (DORNELLES JUNIOR, 2020). Exemplo claro disso se deu na competência da terceira região da Justiça do Trabalho:

> A Justiça do Trabalho determinou que a empresa pague indenização por danos morais a um ex-empregado do setor administrativo que teve seus dados sigilosos expostos no sistema interno de informação da empresa. Um trabalhador da companhia confirmou, no processo que, ao fazer pesquisa no sistema, deparou-se com o relatório médico do autor da ação, com a indicação de que ele tinha pensamentos suicidas e era usuário de cocaína. (DOS SANTOS , 20220, P. 149) (TRIBUNAL REGIONAL DO TRABALHO DA 3ª REGIÃO, 2020)

O legítimo interesse do empregador versus o livre consentimento do empregado.

O livre consentimento (BRASIL, 2018) é um dos pilares jurídicos para coleta, tratamento e cessão de dados pessoais nas legislações mundo afora, porém a primeira questão importante é se seria suficiente para garantir a proteção de direito fundamental à privacidade no ambiente de trabalho. O GDPR europeia, em seu artigo 43, é expresso sobre os riscos do consentimento em situações de desequilíbrio entre as partes.

> art. (43): A fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública pelo que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa. (...). (EUR, 2016)

Porém, na ausência de previsão do tema na LGPD, a doutrina brasileira vem formando esse entendimento semelhante ao estrangeiro, pois os empregadores devem estar atentos não apenas às regras gerais para proteger dados de clientes, fornecedores e parceiros em que há maior ambiente de liberdade. Seu olhar deve ser igualmente cuidadoso e específico quando se trata de dados de empregados os quais, na relação de trabalho, acabam consentindo com a coleta, tratamento e até a cessão de seus dados a terceiros por estarem submetidos ao poder diretivo do empregador. (ZAVANELLA, 2023), (TAVARES, 2023, p. 46).

> O consentimento do trabalhador não é adequado como fundamento de legitimidade para permitir o tratamento de dados pessoais, o fundamento de legitimidade é conferido pela lei laboral, especificamente o n.º 2 do art.º 20.º do Código do Trabalho, que permite em certas circunstâncias a utilização de meios de vigilância à distância no local de trabalho (SILVA, 2020, p. 426) .

Daí outra consequência, com a LGPD em vigor, qualquer solicitação de dados pessoais ou de documentos que contenham informações pessoais de empregado deve se basear em outros pilares de seu artigo 7º, ou seja, por obrigação legal, por necessidade à execução de políticas públicas, para estudos por órgão de pesquisa, para a execução de contrato, para o exercício regular de direitos em processos, para a proteção da vida ou da saúde, para atender aos interesses legítimos do controlador e para a proteção do crédito.

O destaque deve ser dado aos "interesses legítimos", que compõem o segundo mais importante pilar a autorizar a coleta e o tratamento de dados porque pode fazer frente ao consentimento do titular. Evidentemente, se o consentimento do empregado é critério frágil na relação laboral, o legítimo interesse do empregador entra em destaque (CONI JUNIOR; PAMPLONA FILHO, 2021, p. 28)

O legítimo interesse pode vir a se tornar elemento essencial inclusive após a relação de trabalho, quando empregadores se veem diante de obrigações legais de manter informações de ex-empregados por cinco, dez ou até 30 anos (ZAVANELLA, 2023, p. 75), mas não podem tratar ou ceder tais dados sem os devidos cuidados. (SILVA, 2006; ALVES, 2023, p. 103)

O problema é que, na relação de trabalho, sendo o controlador dos dados privativos o próprio empregador, há quem defenda que o "legítimo interesse" do empregador é restrito ou até proibido para outras funções que não aquelas ligadas ao objeto do contrato de trabalho, apenas entre as partes (ZAVANELLA, 2023, p. 116). Para outros, essa legitimidade ficaria sujeita a análises de proporcionalidade e necessidade, sob a luz de uma nova dimensão de "análise de risco" que vem se afirmando como uma das formas de conceber o tratamento e a circulação de dados pessoais sem consentimento informado. (BRUVERE; LOVIC, 2021, p. 2).

A Noção de Análise de Riscos no Legítimo Interesse.

Se o empregador deve assumir papel de protagonista na proteção de dados de seus empregados, deve criar mecanismos para impedir a violação dos dados pessoais de seu próprio pessoal. A criação

dos referidos instrumentos, entretanto, está condicionada ao mapeamento de riscos da atividade desenvolvida pela entidade, no que tange ao tratamento de dados utilizados. As possibilidades de sucesso ou fracasso no tratamento de dados variam sobremaneira em função do tamanho e da atividade desenvolvida. Por exemplo, caso a empresa solicite dados sensíveis dos empregados, deve limitar o acesso a um grupo selecionado de pessoas e possuir controles rígidos para seu acesso, de modo a criar barreiras para seu tratamento, cessão ou vazamento de forma inadvertida, desde que observados os critérios legais para justificar a coleta de dados sensíveis.

Em primeira análise, mapear os riscos nada mais é do que obter uma fotografia da empresa a respeito de onde e como os tratamentos de dados acontecem, para depois, com olhar crítico, criar controles que previnam falhas e, caso estas ocorram, que as medidas corretivas sejam aptas e rápidas para sua identificação, sua correção e mitigação ou reparação dos prejuízos dos titulares de dados. A ideia de mapear os riscos supõe trazer de forma clara, cristalina e quantificada os pontos de atenção que, de alguma forma, podem colocar em risco a atividade de tratamento de dados pessoais dos empregados.

Mas um dos mais interessantes conceitos no tema é a análise de risco em concreto ou a análise específica de risco sobre o legítimo interesse para tratamento de dados caso a caso, tema recente na área, especialmente quando a base de dados é proveniente da relação laboral.

O artigo 10 da LGPD remete à noção de "legitimo interesse", que como vimos é um fundamento que tende a substituir o consentimento em relações assimétricas como a laboral, para ser definida "a partir de situações concretas", dando origem, no Brasil, a um ramo especial de avaliação de risco já presente na área de proteção de dados global a

partir do GDPR (EUR, 2016), que é a avaliação de riscos em legítimo interesse ou "LIA - *Legitimate Interest Assessment"*(ICO, 2018).

Na doutrina nacional, já surgem os primeiros passos dessa "diligência devida" em proteção de dados na relação laboral, comparando as propostas para os testes de "propósito, necessidade e balanceamento" para avaliação de proporcionalidade segundo o princípio de que "quanto maior o risco no tratamento de dados, maior deve ser o legítimo interesse, estimado mediante um teste com etapas, a exemplo de:

> a) Verificação do legítimo interesse com base no caso concreto e da finalidade legítima a que o controlador se propõe (art. 10 da LGPD), devendo ser observado se a coleta promove a atividade do controlador, e, se sim, se essa coleta não é um "cheque em branco". Deve-se analisar, ainda, a situação em concreto para que a regulamentação seja o mais talhada possível ao caso. (...)
> c) Balanceamento entre impactos sobre o titular e as expectativas desse (art. 10, II, da LGPD). Nesse momento, é preciso avaliar se a expectativa de uso do dado que o empregado possui está compatibilizada com o uso procedido (art. 6º, I da LGPD), e, ainda, quais serão as repercussões do uso dos dados no tempo, no espaço e para os titulares em relação aos seus dados, elencando, além dos riscos, os benefícios que podem advir desse tratamento de dados. (ZAVANELLA, 2023, p. 126)

Em conclusão parcial, fica evidente a necessidade de uma atenção aos processos e treinamentos para que uma análise de risco possa ser colocada à prova em avaliação do legítimo interesse para tratamento de dados qualquer que seja o porte ou a natureza pública ou privada do empregador na relação laboral. Essa análise de risco, ou *LIA*, para cumprir o dever legal de avaliação em concreto, pode e deve ser implementada com atenção às distintas fases do contrato de trabalho (CHIAVENATO, 2009). A análise caso a caso, conforme o ramo de atividade, com uma lista de deveres do empregador nas fa-

ses pré-contratual, contratual e pós-contratual é objeto das primeiras reflexões doutrinárias (MELO, 2023).

Considerações finais

Inegável que a proteção de dados pessoais é um dever recente nas relações interpessoais, que, a partir das relações de massa (*big data*) se expandiu para todos os setores da sociedade civil, o que inclui as relações de trabalho. Trata-se de um dever não apenas das empresas, organizações e pessoas físicas, mas também dos empregados que recebem acesso a dados pessoais, haja vista, como se demonstrou, que as sanções administrativas e pecuniárias aos agentes (empregado ou empregador) não se limitam aquelas contidas na LGPD, elas vão além, também por estarmos diante de um direito fundamental.

Em que pese o custo para adaptação a essa nova área regulatória, uma variável deve ser sempre analisada: as sanções administrativas e pecuniárias trazidas pela LGPD são extremamente onerosas, e podem levar, nos casos de violação grave da proteção de dados, à interrupção das atividades econômicas do agente privado que realiza o seu tratamento ou mesmo o encerramento de suas atividades.

As consequências que o tratamento, cessão ou vazamentos inadvertidos de dados pessoais podem trazer na esfera laboral podem ser atribuídas tanto ao empregado, como a dispensa por justa causa, quanto ao empregador, com as principais sanções administrativas, pecuniárias ou não, ou indenizações em processos judiciais, além dos danos reputacionais ou perda de valor de mercado.

Ademais, além da Agência Nacional de Proteção de Dados (ANPD) ter função regulatória geral, na esfera especificamente labo-

ral existe a possibilidade de outros entes estatais instaurarem processos contra o agente de tratamento de dados, como é o caso o MPT e possivelmente sindicatos, como já demonstrado, com pretensão punitiva administrativa, trabalhista, ação civil individual ou ação civil pública (MPT) em caso de suspeitas de descumprimento do dever de proteger os dados dos empregados.

Apesar de todos os riscos mencionados, a proteção de dados pessoais nas relações de trabalho por meio da LGPD deve ser comemorada. A oportunidade de rever conceitos, processos e procedimentos internos significa um salto na qualidade na coleta e tratamento de informações pessoais, bem como a racionalização sobre quais são essenciais ou necessárias na base de avaliação de riscos.

Por último a realização de auditorias é ferramenta fundamental para que se verifique a real dimensão do risco, a avaliação do legítimo interesse em tratamento de dados, conforme a natureza da organização, o ramo de atividade, o tamanho e outros critérios que permitem aumento da transparência e do dever de diligência nas relações jurídicas em concreto, especialmente empresariais, como determinam os principais padrões de conduta disponíveis nesta intersecção de áreas regulatórias.

Referências

ARAUJO, Luiz Alberto David; NUNES JÚNIOR, Vidal Serrano. **Curso de direito constitucional**, 3ª ed., São Paulo, Saraiva, 2007, p. 71 e 72.

BIDERMAN, Ciro et al. Big data para o desenvolvimento urbano sustentável: criando políticas públicas urbanas baseadas em evidências. **BID/FGV**, 2021.

BIONI, Ricardo Bruno. **Proteção de Dado Pessoais: a função e os limites do consentimento**. 1ª ed., Rio de Janeiro: Forense, 2019.

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. **Planalto.** Recurso on line. Disponível em: https://www.planalto.gov.br/ Acesso em: 04/07/2024.

BRASIL, Consolidação das Leis do Trabalho. Decreto-Lei Nº 5.452, de 1º de maio de 1943. **Planalto.** Recurso on line. Disponível em: https://www.planalto.gov.br/ Acesso em: 04/07/2024.

BRASIL, Lei Nº 13.709 de 14 de agosto de 2018. **Planalto.** 2018. Recurso on line. Disponível em: https://www.planalto.gov.br/ Acesso em: 04/07/2024.

BRASIL. Tribunal Superior do Trabalho. Agravo de Instrumento em Recurso de Revista 20954-25.2019.5.04.0015, Relator Ministro Mauricio Godinho Delgado; 02/07/2021). **TST.** Recurso on line. Disponível em: https://www.tst.jus.br/jurisprudencia Acesso em: 04/07/2024.

BRUVERE, Anna; LOVIC, Victor. Rethinking Informed Consent in the Context of Big Data. **Cambridge Journal of Science and Policy**. doi:10.17863/CAM.68396.2021.

CASTELLS, Manuel. **A sociedade em rede.** São Paulo: Paz e Terra, 1999

CHIAVEGATTO FILHO, Alexandre Dias Porto. Uso de big data em saúde no Brasil: perspectivas para um futuro próximo. **Epidemiologia e Serviços de Saúde**, v. 24, p. 325-332, 2015.

CHIAVENATO, Idalberto. **Recursos Humanos:** O capital das organizações. 9 ed. Revista e Atualizada. Rio de Janeiro: Elsevier, 2009.

COE. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**, 2018. Disponível em: https://www.coe.int/en/web/data-protection/convention108-and-protocol acesso em: 07 de junho de 2024.

CONI JUNIOR, Vicente. Vasconcelos; PAMPLONA FILHO, Rodolfo . A Lei Geral de Proteção de Dados Pessoais e os impactos no ônus da prova no processo do trabalho brasileiro. **Revista LTr**. Legislação do Trabalho, v. 7, 2021.

CORBET , et al. The Ruling in Schrems II. **Arthurcox.com.** Irlanda, 24 jul. 2020. Disponível em: https://www.arthurcox.com/knowledge/the-ruling-in-schrems-ii/ Acesso em: 01/07/2024.

DIDDIER JR., Fredie; ZANETI JR., Hermes. **Curso de Direito Processual Civil**, Processo Coletivo, v. 4, 4. Ed., Salvador, Editora Juspodivm, 2009.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. São Paulo: Revista dos Tribunais, 2021.

DORNELLES JUNIOR, Paulo Roberto. Sentença. Negativa de acesso a dados pessoais tratados (art. 9º da LGPD) *In:* Barzotto, Luciane Cardoso e Costa, Ricardo H. Martins. **Estudos sobre a LGPD - Lei Geral de Proteção de Dados**: doutrina e aplicabilidade no âmbito laboral (Artigos, Decisões & Glossário). - Porto Alegre : Escola Judicial do Tribunal Regional do Trabalho da 4ª Região. Diadorim Editora, 2022.

DOS SANTOS, Flávia Alcassa; LIMA, Adrianne. A relação trabalhista sob o viés da proteção de dados e privacidade: due diligence de candidatos e empregados, incidentes com dados pessoais e possível reparação a danos. In: *In:* Barzotto, Luciane Cardoso e Costa, Ricardo H. Martins. **Estudos sobre a LGPD - Lei Geral de Proteção de Dados**: doutrina e aplicabilidade no âmbito laboral (Artigos,

Decisões & Glossário). - Porto Alegre : Escola Judicial do Tribunal Regional do Trabalho da 4ª Região. Diadorim Editora, 2022.

EFF. **Electronic Frontier Foundation Annual Report 2022**. EFF. org. 2022.

EUR-Lex. Data Protection Directive (95/46/EC). Directiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de Outubro de 1995. **União Europeia**. Recurso digital. Disponível em https://eur-lex.europa.eu/ Acesso em: 04/07/2024.

EUR-Lex. GDPR – *General Data Protect Regulation / Regulamento Geral sobre a Proteção de Dados*. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016. **União Europeia**. Recurso digital. Disponível em https://eur-lex.europa.eu/ Acesso em: 04/07/2024.

FERNÁNDEZ, Yarina Amoroso; FERRER, Dévorah Costales. Big Data: una herramienta para la administración pública. **Ciencias de la Información**, v. 47, n. 3, p. 3-7, 2016.

FERREIRA, Vanessa Rocha; FALCÃO, Beatriz Normando; BIZZOCCHI, Lucas Jorge João. Digital, Privacidade e Proteção de Dados: uma análise dos Impactos da LGPD no Direito do Trabalho. **Revista Conjectura**, Vol. 22, nº 2, p. 219-241, 2022.

FREITAS, Carla Maria Dal Sasso; PIMENTA, Marcelo Soares. Big data, visualização de informações e visual analytics em suporte a políticas públicas. **Governança digital** [recurso eletrônico]. 1. ed. Porto Alegre, RS: Ed. da UFRGS, 2014.

G1. Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber. **Portal G1**, [s. l.], Economia, Tecnologia, 28 jan. 2021. Disponível em: https://glo.bo/3vyrS1L. Acesso em: 24 jun. 2024

GAIATO, Kris. Cambridge Analytica teria atuado no Brasil nas últimas eleições. **Tecmundo**. 09 jan. 2020. Disponível em: <https://www.tecmundo.com.br/seguranca/149120-cambridge-analytica-teria-atuado-brasil-ultimas-eleicoes.htm>. Acesso em: 05 de junho 2022.

ICDPPC. **Declaration on Ethics and data protection in artificial intelligence: 40th International Conference of Data Protection and Privacy Commissioners**. 23 de outubro de 2018. Disponível em: https://globalprivacyassembly.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf; acesso em: 08 de abril de 2024.

ICO. Information Commissioner's Office. **Guide to the General Data Protection Regulation (GDPR)**. 2018. Item: "How can we apply legitimate interests in practice?".

ILO INTERNATIONAL LABOUR ORGANIZATION. **Protection of workers' personal data**. An ILO code of practice. Geneva, ILO, 1997.

MARCELINO, Danielle Alves Correia et al. Comercialização de dados pessoais sob a óptica do ordenamento jurídico brasileiro: uma análise do caso da empresa de serviços de assessoria sa (Serasa Experian). **Revista Foco**, v. 17, n. 5, p. e5267-e5267, 2024.

MELO, Mariana de Araújo. **Breve análise da Lei Geral De Proteção De Dados (LGPD) e seus principais impactos nas relações de trabalho**. Monografia. UFPE. 2023.

NAIR, Meghna Manoj; TYAGI, Amit Kumar. Privacy: History, Statistics, Policy, Laws, Preservation and Threat Analysis. **Journal of Information Assurance & Security**, v. 16, n. 1, 2021.

NYT. Facebook Puts Profile Breach At 87 Million. **NYT.** April 5, 2018, Page A1. Disponível em <https://www.nytimes.

com/2018/04/04/technology/mark-zuckerberg-testify-congress.html> acesso em: 08 de maio de 2024.

OCDE. **Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais**. OCDE, 2003. Disponível em: https://www.oecd.org/sti/ieconomy/15590254.pdf. Acesso em: 28 de fevereiro 2024.

PALMER, Michael. Data is the New Oil. **ANA Blog**. 2006.

PRIVACY INTERNATIONAL; DCAF – GENEVA CENTRE FOR SECURITY SECTOR**. Understanding private surveillance providers and technologies: within the wider framework of private security governance**. s/d. Disponível em: <https://privacyinternational.org/sites/default/files/2024-02/DCAF_PI_Understanding%20Private%20Surveillance_WEB.pdf> acesso em 20 de abril de 2024.

RAUTENBERG, Sandro; CARMO, Paulo Ricardo Viviurka do. Big Data e Ciência de Dados: complementariedade conceitual no processo de tomada de decisão. **Brazilian Journal of Information Studies**: Research Trends. 13:1 (2019).

RUSTAD, Michael L. and KOENIG, Thomas H. Towards a Global Data Privacy Standard, 71 **Fla. L. Rev**. 365.

SILVA, Fabrício Lima. LGPD nas relações de trabalho: os riscos de utilização do consentimento para o tratamento dos dados dos trabalhadores. In: DOS SANTOS, Flávia Alcassa. A lei geral de proteção de dados pessoais (LGPD) e a exposição de dados sensíveis nas relações de trabalho. **Revista do Tribunal Regional do Trabalho da 10ª Região**, v. 24, n. 2, 2020

SILVA, Leda Maria Messias. Poder diretivo do empregador, emprego decente e direitos da personalidade. **Revista Jurídica Cesumar**, v. 6, n. 1, p. 267-281, 2006.

SILVA, Leda Maria Messias; ALVES, Nadine Girardi. LGPD e compliance: a efetivação dos direitos da personalidade nas relações de emprego. **Scientia Iuris**, v. 27, n. 2, 2023.

SOUZA, Marcelo Silveira De. **O papel do Ministério Público no enforcement da Lei Geral de Proteção de Dados e demais desdobramentos da aprovação da LGPD no judiciário brasileiro.** TCC. IDP, Brasília, 2021. Disponível em: http://52.186.153.119/bitstream/123456789/3642/1/TCC_%20MARCELO%20SILVEIRA%20DE%20SOUZA%20_2020.pdf Acesso em 01 de junho de 2024.

TAN, Pang-Ning; STEINBACH, Michael; KUMAR, Vipin. **Introduction to data mining**. Pearson Education, India, 2016.

TAVARES, Lara Rodrigues de Queiroz. **Tratamento de dados pessoais no contexto das relações de trabalho**: o vício do consentimento do empregado. Trabalho de Conclusão de Curso. UFPE. 2023

TÉLLEZ CARVAJAL, Evelyn. Análisis documental respecto al análisis de grandes cúmulos de datos (Big Data) en materia de Derechos Humanos. **Revista de la Facultad de Derecho de la Pontificia Universidad Católica del Perú**, núm 84, p. 155-188, 2020.

TRIBUNAL REGIONAL DO TRABALHO DA 3ª REGIÃO. Copasa deverá indenizar trabalhador por exposição de dados na rede interna de informações da empresa. Belo Horizonte: **TRT3**, 01º julho 2020. Disponível em: https://portal.trt3.jus.br/internet/conheca-o-trt/comunicacao/noticias-juridicas/nj-copasa-devera-indenizar-trabalhador-por-exposicao-de-dados-pessoais-na-rede-interna-de-informacao-da-empresa. Acesso em: 20 fev. 2024

UN. **The right to privacy in the digital age**. Res. 71/199. General Assembly. 2017

ZAVANELLA, Fabiano. **Aplicação da Lei Geral de Proteção de Dados nas relações trabalhistas: limites do consentimento do empregado e do legítimo interesse do empregador**. 2023. Tese (Doutorado) – Universidade de São Paulo, São Paulo, 2023.