UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO (UNIRIO)

CENTRO DE CIÊNCIAS JURÍDICAS E POLÍTICAS (CCJP)

ESCOLA DE CIÊNCIAS JURÍDICAS

BEATRIZ MARINHO JORGE

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E AS RELAÇÕES DE TRABALHO

Rio de Janeiro

2022

BEATRIZ MARINHO JORGE

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E AS RELAÇÕES DE TRABALHO

Trabalho de Conclusão de Curso apresentado à Escola de Ciências Jurídicas da Universidade Federal do Estado do Rio de Janeiro como requisito parcial à obtenção do grau de Bacharel em Direito.

Profª. Drª. Carolina Tupinambá

Rio de Janeiro

2022

Marinho Jorge, Beatriz
M82 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E AS RELAÇÕES DE TRABALHO / Beatriz Marinho Jorge. -- Rio de Janeiro, 2022.
61

Orientador: Carolina Tupinambá.
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal do Estado do Rio de Janeiro, Graduação em Direito, 2022.

1. LGPD. 2. Relações de Trabalho. I. Tupinambá, Carolina, orient. II. Título.

BEATRIZ MARINHO JORGE

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E AS RELAÇÕES DE TRABALHO

Trabalho de conclusão de curso apresentado à Escola de Ciências Jurídicas da Universidade Federal do Estado do Rio de Janeiro como requisito parcial à obtenção do grau de Bacharel em Direito.

Rio de Janeiro, 17 de agosto de 2022.

Banca Examinadora

_____

Profª. Drª. Carolina Tupinambá

Universidade Federal do Estado do Rio de Janeiro

_____

Prof. Dr. Daniel Queiroz Pereira

Universidade Federal do Estado do Rio de Janeiro

_____

Prof. Dr. Fábio Rodrigues Gomes

Universidade do Estado do Rio de Janeiro

Rio de Janeiro

2022

Dedico este trabalho a todos que me apoiaram até aqui – minha família como um todo, compreendendo também amigos e namorado (a família que escolhi) – para que eu pudesse alçar vôos cada vez mais altos. Dedico especialmente aos meus pais, que vibram com todas as minhas conquistas como se fossem suas, porque são também.

AGRADECIMENTOS

Agradeço, em primeiro lugar, à Deus, por escrever todo meu caminho e permitir que eu tenha coragem, determinação e intuição para segui-lo diariamente.

Agradeço ao meu pai, Eduardo, por seu meu maior exemplo de ser humano e cidadão, por sempre me dar afeto, ouvidos, risadas, cerveja e doce de leite. Agradeço à minha mãe, Janete, pela herança da espontaneidade, carisma e jogo de cintura tão necessários para a vida, e também pelo colo para o qual eu sempre posso voltar. Eu amo vocês mais do que poderia escrever.

Ao meu companheiro de rotina, passeios, sonhos, planos, de tudo: Matheus. Você é a pessoa mais linda que eu poderia encontrar nessa e em qualquer outra vida, e sem você essa jornada com certeza teria sido muito mais difícil. Obrigada por nós.

Aos meus irmãos, Eduardo e Pedro, pela parceria e pela certeza de que nunca estarei sozinha. Muito obrigada pela dose certa de estresse, amor e companheirismo. Sem esse equilíbrio perfeito provavelmente já teríamos nos matado.

À toda minha família – pais, irmãos, madrasta, tios, primos e avós –, que possui a dádiva de levar a vida de forma leve, com humor e muita risada, mesmo quando a tristeza invade. Agradeço pelas alegrias compartilhadas e pela convicção de que sempre teremos uns aos outros.

Agradeço também a quem já não está mais aqui, mas que, ainda assim, sempre estará. Em especial, agradeço ao meu tio Márcio Chaulfun Jorge por todos os momentos compartilhados em família e por sua luz, que jamais serão esquecidos.

Agradeço aos meus colegas de trabalho da Equinor Brasil, por acreditarem em mim e impulsionarem meu desenvolvimento profissional dia após dia.

Agradeço aos meus amigos queridos da UNIRIO, vocês são mais do que eu poderia esperar. Muito obrigada pelos bares, festas, piadas, fofocas e, claro, aulas compartilhadas.

Incluo nesse agradecimento também meus animais de estimação – Madalena, Filomena e Koda, pela companhia fiel e amor incondicional.

“Amar e mudar as coisas me interessa mais.”

Belchior

RESUMO

O presente estudo analisa a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) – e suas implicações nas relações de trabalho. Mais especificamente, busca-se entender as particularidades de sua aplicação e seus impactos já percebidos e esperados daqui para frente nas relações trabalhistas. Considerando a contemporaneidade da LGPD e a "recente" estruturação da Agência Nacional de Proteção de Dados (ANPD), o presente trabalho também discorrerá sobre os principais pontos nebulosos no que tange à proteção de dados pessoais no direito brasileiro, com enfoque nas relações de trabalho, buscando referencial na aplicação da *General Data Protection Regulation* (GDPR), da União Europeia – inspiração para a LGPD. A partir da revisão bibliográfica, este estudo propõe-se a traçar um panorama dos efeitos da LGPD no direito trabalhista pátrio, com enfoque nas principais especificidades de sua aplicação nas relações de trabalho, à luz do que já se pôde observar desde o início da vigência da LGPD, da atuação da ANPD, da aplicação da GDPR, bem como da atuação das autoridades europeias de proteção de dados pessoais.

Palavras chave: Contrato de Trabalho; Relações de emprego; privacidade; ANPD; GDPR.

ABSTRACT

This paper analyzes Law No. 13,709/2018 – the General Data Protection Law (LGPD) – and its implications in labor relations. More specifically, it seeks to understand the particularities of its application and impacts already perceived and expected going forward in employment relations. Considering the contemporaneity of the LGPD and the "recent" structuring of the National Data Protection Agency (ANPD), the present work will also discuss the main nebulous points regarding the protection of personal data in Brazilian law, focusing on labor relations, seeking reference in the application of the General Data Protection Regulation (GDPR), of the European Union – inspiration for the LGPD. Through literature review, this study aims to outline an overview of the LGPD's effects in national labor law, focusing on the main specificities of its application in labor relations, in the light of what has already been observed since the beginning of the LGPD's term, the performance of ANPD, and what could be extracted from the application of the GDPR, as well as the performance of European data protection authorities.

Key words: Employment agreement; employment relations; privacy; ANPD; GDPR.

SUMÁRIO

INTRODUÇÃO

O instituto da proteção de dados pessoais no Brasil tem origem muito anterior à promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD ou Lei nº 13.709/2018)[1]. Os preceitos e princípios da LGPD não se concentraram em uma lei geral de proteção de dados da noite para o dia – essa centralização se dá a partir de diversos dispostivos, leis, normas e regulamentos sobre o tema dispersos no quadro jurídico brasileiro desde a Carta Magna.

A Constituição Federal de 1988[2] traz, em seu artigo 5º, inciso X, a proteção à vida privada e à intimidade no rol de direitos fundamentais. De certa forma, a proteção de dados encontra uma de suas primeiras tutelas em tal dispositivo, vindo a evoluir até 2022, quando, por meio da Emenda Constitucional nº 115[3], reconheceu-se expressamente a proteção aos dados pessoais, inclusive nos meios digitais, como direito fundamental do cidadão brasileiro.[4]

Também trata da proteção aos dados pessoais o Código Civil (CC)[5], através da tutela dos direitos da personalidade (arts. 11 a 21 do CC). Segundo Bruno Ricardo Bioni (2021, p. 52), o rol de direitos da personalidade previsto no Código Civil não é taxativo, o que permite o reconhecimento da proteção de dados pessoais como um direito da personalidade.

Até a publicação da LGPD, a Lei nº 12.965/2014 (Marco Civil da Internet) [6] era o que tínhamos de mais concreto em termos de proteção aos dados pessoais no quadro normativo brasileiro, trazendo conceitos e princípios que agora encontram-se concretizados na Lei nº 13.709/2018, como em seu artigo 7º, inciso VII, que menciona a possibilidade de fornecimento

---

[1] BRASIL. Lei nº 13.709/2018. Lei Geral de Proteção de Dados Pessoais. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 07 de maio de 2022.

[2] BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 07 de maio de 2022.

[3] BRASIL. Emenda Constitucional nº 115/2022. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 07 de maio de 2022.

[4] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
(...)
X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
(...)
LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

[5] BRASIL. Lei nº 10.406/2002. Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 07 de maio de 2022.

[6] BRASIL. Lei nº 12.965/2014. Marco Civil da Internet. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 07 de maio de 2022.

a terceiros dos dados pessoais dos usuários da Internet, exceto mediante consentimento, que deverá ser livre, expresso e informado, ou nas demais hipóteses previstas em lei.[7]

Não busca-se nesta introdução traçar uma linha do tempo exata acerca da tutela de dados pessoais no ordenamento jurídico brasileiro, mas tão somente demonstrar que o tema não veio exatamente como novidade na LGPD.

Na verdade, pode-se dizer que a LGPD centralizou conceitos, preceitos e princípios que já encontravam alguma raíz no quadro normativo pátrio. No entanto, sua entrada em vigor encontrou alguns percalços, e é inegável dizer que a "nova" lei geral de proteção de dados trouxe impactos significativos, tanto para os cidadãos brasileiros, quanto para o mercado nacional.

A LGPD foi promulgada em 14 de agosto de 2018 e, a princípio, sua *vacatio legis* se encerraria em 14 de fevereiro de 2020, dezoito meses após sua promulgação. No entanto, considerando as grandes mudanças que a aludida norma demandou, a necessidade de mais tempo para que as empresas e órgãos públicos se adequassem aos requisitos impostos e, ainda, a subsequente crise ocasionada pela pandemia do vírus SARS-CoV-2 (Covid-19), iniciada em março de 2020, através da Medida Provisória nº 959, de 29 de abril de 2020[8] – posteriormente convertida na Lei nº 14.058/2020[9] –, buscou-se a extensão da vacância da lei para maio de 2021.

No entanto, o Senado Federal vetou o dispositivo da Medida Provisória nº 959 que previa a prorrogação do prazo para entrada em vigor das principais disposições da LGPD e, após a referida MP ser sancionada pela Presidência da República, a Lei Geral de Proteção de Dados Pessoais entrou em vigor em 18 de setembro de 2020.

Com as crises sanitária e econômica decorrentes da Covid-19 ainda muito acentuadas no Brasil, publicou-se, em junho de 2020, a Lei nº 14.010[10], que, dentre outras previsões, alterou o artigo 65 da Lei nº 13.709/2018 para acrescentar o inciso I-A, determinando que os artigos

---

[7] "Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
(...)
VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;"

[8] BRASIL. Medida Provisória nº 959, de 29 de abril de 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv959.htm. Acesso em: 07 de maio de 2022.

[9] BRASIL. Lei nº 14.058, de 17 de setembro de 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Lei/L14058.htm. Acesso em: 07 de maio de 2022.

[10] BRASIL. Lei nº 14.010/2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14010.htm. Acesso em: 07 de maio de 2022.

52, 53 e 54 da referida lei – que dispõem sobre as sanções administrativas – somente entrariam em vigor em 01 de agosto de 2021.

Assim, as empresas e órgãos públicos puderam se planejar para instituírem em suas organizações internas projetos de adequação à "nova" lei geral de proteção de dados, para que, finalmente, em 01 de agosto de 2021, quando passaram a valer as sanções administrativas previstas na LGPD, estivessem em conformidade com os requisitos impostos pela referida lei.

Por se tratar de um assunto relativamente novo para o cenário brasileiro, há muitas incertezas sobre a regulamentação da LGPD e a atuação da Autoridade Nacional de Proteção de Dados (ANPD) – órgão da Administração Pública instituído pela Medida Provisória nº 869, de 27 de dezembro de 2018[11], convertida na Lei nº 13.853, de 14 de agosto de 2019[12] – na fiscalização da lei.

A ANPD, conforme mencionado acima, foi criada em 2018, mas sua estrutura regimental foi instituída através da publicação do Decreto nº 10.474, de 26 de agosto de 2020[13], com entrada em vigor somente na data de publicação da nomeação do Diretor-Presidente da ANPD no Diário Oficial da União, o que se deu em 06 de novembro de 2020[14].

Contudo, apesar das sanções adminitrativas terem entrado em vigor somente em 2021, as empresas e órgãos públicos tiveram que, desde agosto de 2020, estruturarem-se para estar em conformidade com as demais previsões da LGPD. Isso porque já poderiam ser demandadas judicialmente pelos titulares de dados pessoais desde a entrada em vigor das principais disposições da lei.

Como se observa, a LGPD trouxe, desde sua publicação, grandes impactos aos negócios brasileiros. No entanto, a necessidade de se ter uma lei geral de proteção de dados pessoais justifica-se não somente pela garantia de direitos aos cidadãos brasileiros, mas também, e em caráter significativo, pelos anseios econômicos do mercado nacional.

Segundo Caitlin Mulholland e Isabella Z. Frajhof (2020, p. 12), um dos propósitos de se ter uma lei geral de proteção de dados no Brasil foi a intenção de ingresso do país na

---

[11] BRASIL. Medida Provisória nº 869, de 27 de dezembro de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869.htm. Acesso em: 07 de maio de 2022.

[12] BRASIL. Lei nº 13.853/2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 07 de maio de 2022.

[13] BRASIL. Decreto nº 10.474/2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10474.htm. Acesso em: 07 de maio de 2022.

[14] Em 06 de novembro de 2020, houve a publicação, pela Casa Civil, dos decretos de 05 de novembro de 2020 que nomearam os Diretores e o Diretor-Presidente da ANPD. Disponível em: https://www.in.gov.br/web/dou/-/decretos-de-5-de-novembro-de-2020-286734594. Acesso em: 07 de maio de 2022.

Organização para a Cooperação e Desenvolvimento Econômico (OCDE). Isso porque um dos requisitos para entrada na OCDE é que o país tenha um arcabouço legal que endereçe a proteção de dados pessoais.

Além disso, a LGPD veio como um mecanismo imprescindível para o mercado brasileiro, uma vez que diversas empresas internacionais, em especial as localizadas na União Europeia, estão sujeitas à normas que estabelecem que a transferência internacional de dados só poderá ser feita para países que possuam um sistema jurídico sólido de proteção de dados.

É o caso, por exemplo, da General Data Protection Regulation (GDPR)[15], da União Europeia, que determina, em seu artigo 45, que a transferência de dados pessoais para países terceiros ou organismos internacionais só poderá ocorrer em casos em que a comissão (órgão europeu responsável por assegurar a proteção dos direitos e liberdades dos indivíduos relacionados ao tratamento de seus dados pessoais) entenda que tal país, território ou um ou mais setor específico dentro de tal país tenha um nível adequado de proteção de dados. Tal nível de proteção é aferido à luz de diversos fatores, como a existência de um sistema jurídico de proteção de dados e de uma autoridade fiscalizadora, por exemplo.

Não por coincidência, a LGPD muito se aproxima da GDPR, uma vez que o regulamento europeu foi forte inspiração para a criação da lei geral de proteção de dados brasileira. Assim, muitos conceitos e interpretações trazidas pela GDPR podem ser encontrados na LGPD. Na verdade, há mais semelhanças do que diferenças entre os dois textos legais, e também é objeto do presente trabalho analisar pontos específicos de convergência e divergência entre ambos.

Ainda que, conforme abordado acima, tenha havido fortes motivações comerciais para a criação de uma lei geral de proteção de dados brasileira, é inegável que a LGPD mostra-se como um grande avanço social para o país, consolidando direitos, agora fundamentais, dos cidadãos, e impondo, ao mesmo passo, deveres às empresas e órgãos públicos no tocante ao tratamento de dados pessoais de pessoas naturais que sejam seus clientes, empregados, servidores, colaboradores, etc.

Não obstante a natural e quase inevitável correlação que se faz entre a Lei Geral de Proteção de Dados Pessoais e o direito consumerista, o presente estudo busca analisar os impactos da LGPD no direito do trabalho. Nessa seara, procura-se entender quais implicações a LGPD

[15] UNIÃO EUROPEIA. Regulação nº 679/2016: General Data Protection Regulation (GDPR). Disponível em: https://gdpr-info.eu/. Acesso em: 07 de maio de 2022.

trouxe para as relações trabalhistas, e quais especificidades surgem nesse cenário, à luz de três pilares da LGPD: (i) os princípios; (ii) as hipóteses de tratamento de dados pessoais; e (iii) os direitos dos titulares.

1. A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS BRASILEIRA

Como adiantado no capítulo introdutório da presente monografia, a Lei nº 13.709/2018 surgiu em um contexto no qual já não se podia ignorar a necessidade de se ter uma lei geral de proteção de dados pessoais no ordenamento jurídico brasileiro. Ainda que o Brasil não possuísse uma cultura de proteção de dados forte até então, a promulgação da LGPD vem trazido, aos poucos, maior conscientização aos cidadãos sobre a necessidade de tutela de seus dados e privacidade.

A Comissão de Assuntos Econômicos do Senado Federal (CAE), por meio de relatório legislativo sob o nº SF/18341.29177-00, de 29 de junho de 2018, de relatoria do Senador Ricardo Ferraço, atribuiu a necessidade de um marco regulatório de proteção de dados ao fato de que o dado pessoal é "hoje, o principal insumo da economia globalizada e baseada em tecnlogia".

Assim, e em linha com o que se pode extrair do capítulo anterior, os dados são considerados uma *commodity* cada vez mais valiosa, e, consequentemente, sua tutela ganha mais importância.

No entanto, apesar de inquestionável a importância da Lei Geral de Proteção de Dados Pessoais, há diversas lacunas ainda não preenchidas e pontos ainda nebulosos quanto à sua aplicação e fiscalização pela ANPD.

Não obstante, o caminho desse marco regulatório até aqui já reflete um grande avanço para a sociedade brasileira, estabelecendo normas e parâmetros a serem observados quando do processamento de dados pessoais, baseando-se em três principais alicerces: (i) os princípios; (ii) as hipóteses de tratamento de dados pessoais; e (iii) os direitos dos titulares.

1.1.OS PRINCÍPIOS DA LGPD

Antes de entrar especificamente nos princípios da LGPD, vale traçar um breve panorama dos princípios gerais de proteção de dados pessoais.

Sabe-se que o instituto da proteção de dados abarca o direito à privacidade, mas não se limita a ele. Isso porque nem todos os dados pessoais são confidenciais, o que não significa dizer que dados pessoais públicos estão fora do círculo de proteção da LGPD.

A necessidade de tutela da privacidade e proteção de dados avança ao passo que a internet se torna o principal meio de comunicação e transmissão de dados. Já em 1973, pouco depois da criação da internet nos Estados Unidos[16], um relatório elaborado pelo Comitê Consultivo sobre Sistemas Automatizados de Dados Pessoais da Secretaria de Saúde, Educação e Bem-Estar dos Estados Unidos (Secretary of Health, Education, and Wealfare) já dava conta de alguns princípios presentes hoje no instituto da proteção de dados.

No relatório, o Comitê afirma que

> A privacidade pessoal de um indivíduo é diretamente afetada pelo tipo de divulgação e uso feito de informações identificáveis registradas a seu respeito. Um registro contendo informações sobre um indivíduo de forma identificável deve, portanto, ser regulada por procedimentos que garantam ao indivíduo o direito de participar das decisões relacionadas ao conteúdo dos registros, e quais divulgações e usos serão feitos sobre suas informações identificáveis nesse registro. Qualquer registro, divulgação e uso de informações pessoais identificáveis não reguladas por tais procedimentos devem ser entendidas como uma prática informacional injusta, a menos que tal registro, divulgação ou uso sejam especificamente autorizados por lei. (**tradução nossa**)[17]

Ademais, o Comitê traçou algumas recomendações em linha com a formulação acima. Vejamos:

- Não deve haver sistemas de registro de dados pessoais cuja própria existência é secreta.
- Deve haver uma maneira de um indivíduo descobrir que informações sobre ele estão em um registro e como elas são utilizadas.
- Deve haver uma maneira de um indivíduo evitar que informações sobre ele que foram obtidas para um propósito sejam usadas ou disponibilizadas para outros fins sem o seu consentimento.
- Deve haver uma maneira de um indivíduo corrigir ou alterar um registro de informações identificáveis sobre ele.

[16] Em 1969 a primeira mensagem teria sido trocada entre dois computadores por meio de seus IMPs complementares. A chamada "Arpanet" pertencia ao Departamento de Defesa dos Estados Unidos e fora desenvolvida no contexto da Guerra Fria, para uso militar. Disponível em: https://www.bbc.com/portuguese/geral-50162526; https://www.ebiografia.com/quem_criou_internet/. Acesso em 11 de junho de 2022.

[17] "An individual's personal privacy is directly affected by the kind of disclosure and use made of identifiable information about him in a record. A record containing information about an individual in identifiable form must, therefore, be governed by procedures that afford the individual a right to participate in deciding what the content of the record will be, and what disclosure and use will be made of the identifiable information in it. Any recording, disclosure, and use of identifiable personal information not governed by such procedures must be proscribed as an unfair information practice unless such recording, disclosure or use is specifically authorized by law." E.U.A., *Records, computers and the rights of citizens.* Report of the Secretary's Advisory Committee on Automated Personal Data Systems, 1973. Disponível em: https://aspe.hhs.gov/reports/records-computers-rights-citizens. Acesso em 11 de junho de 2022.

- Qualquer organização que crie, mantenha, use ou divulgue registros de dados pessoais identificáveis deve garantir a confiabilidade dos dados para o uso pretendido e deve tomar precauções para evitar o uso indevido dos dados. (**tradução nossa**)[18]

Desse modo, é possível observar a existência de princípios de privacidade e proteção de dados mundo afora muito antes de qualquer discussão no Brasil sobre a criação de uma lei geral de proteção de dados.

Tais elementos norteadores, presentes hoje na LGPD, encontram, portanto, origem no ordenamento jurídico estrangeiro, e são comuns aos modelos internacionais de privacidade e proteção de dados.

Das recomendações do Comitê Consultivo sobre Sistemas Automatizados de Dados Pessoais elencadas acima, pode-se extrair os seguintes princípios da Lei Geral de Proteção de Dados Pessoais: (i) transparência; (ii) livre acesso; (iii) finalidade; (iv) adequação; (v) qualidade dos dados; (vi) prevenção e; (vii) segurança, todos presentes nos incisos do artigo 6º da Lei nº 13.709/2018.

Não estão restritos, no entanto, e conforme já pincelado acima, ao ordenamento jurídico brasileiro, estando presentes no instituto da proteção de dados global desde a publicação da Convenção 108 do Conselho da Europa[19] e das Guidelines da OCDE[20] (DONEDA, 2019, p. 181).

- [18] "There must be no personal data record keeping systems whose very existence is secret.
- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data." Idem.

[19] "A Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, de 28 de janeiro de 1981, foi o primeiro instrumento internacional juridicamente vinculativo adotado no domínio da proteção de dados." Disponível em: https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf. Acesso em 12 de junho de 2022.

[20] Os *Guidelines* da OCDE em proteção de dados foram elaborados para estabelecer padrões mínimos a serem complementados por medidas adicionais de proteção de dados e privacidade e liberdades individiuais em cada país. Os *Guidelines* foram divulgados em 1980 e atualizados em 2013. Disponível em: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#preface. Acesso em 12 de junho de 2022.

Tais princípios, em adição aos demais aludidos na LGPD – da necessidade; da não discriminação; e da responsabilização e prestação de contas –, constituem um conjunto de normas que devem reger o tratamento de dados pessoais, de forma a garantir transparência e conformidade com a lei.

1.2. AS HIPÓTESES LEGAIS DE TRATAMENTO DE DADOS PESSOAIS

Com a ascensão do instituto da proteção de dados pessoais no Brasil, muitas empresas temeram ter seus negócios impactados negativamente com a possibilidade de interrupção das atividades de tratamento de dados pessoais.

No entanto, ao contrário do que se pode pensar, a Lei nº 13.709/2018 não surgiu com o objetivo de proibir todo e qualquer tipo de atividade de tratamento de dados pessoais, mas sim de regular e viabilizar tais atividades de forma segura e observando os direitos e liberdades do titular dos dados.

Nesse sentido, o artigo 7º da LGPD elenca as hipóteses nas quais o tratamento de dados pessoais pode ocorrer, quer sejam:

> I - mediante o fornecimento de consentimento pelo titular;
>
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
>
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
>
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
>
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
>
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
>
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
>
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
>
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
>
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Ainda, quando o tratamento estiver ligado a um dado pessoal sensível, as hipóteses nas quais tal tratamento pode ocorrer são ainda mais restritas, estando listadas no artigo 11 da LGPD:

> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
>
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
>
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
>
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
>
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
>
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
>
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
>
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

A definição de uma hipótese é o primeiro passo para que o tratamento de dados pessoais seja considerado legal. Sendo assim, resta clara a importância das bases legais trazidas pela LGPD – são justamente o respaldo que o controlador e o operador possuem para tratar dados pessoais.

Mesmo porque a criação de uma lei geral de proteção de dados pessoais que restringisse por completo as atividades de tratamento não estaria em harmonia com um dos principais fatores que impulsionaram a criação da LGPD: a viabilização da atuação de empresas brasileiras internacionalmente, considerando os demais regulamentos mundo afora que restringem a transferência de dados para países que não possuem um sistema jurídico sólido regulamentando o tema.

Ademais, é importante que o controlador e operador tenham registro das bases legais utilizadas, de forma a garantir a transparência da atividade de tratamento de dados pessoais, deixando claro para o titular qual hipótese prevista na LGPD autoriza determinado tratamento.

1.3. DIREITOS DOS TITULARES DE DADOS PESSOAIS

Pelo próprio contexto da criação da LGPD, pode-se dizer que ela tem sido interpretada muito mais como uma nova obrigação para as empresas e organizações do que como um novo direito dos cidadãos brasileiros.

O reconhecimento da proteção de dados pessoais como um direito fundamental, com a inclusão do inciso LXXIX no artigo 5º da Constituição Federal, veio para reforçar esse outro lado da LGPD – o dos direitos dos titulares.

O artigo 18 da Lei nº 13.709/2018 enumera os direitos dos titulares, em linha com as obrigações do controlador perante o titular:

> I - confirmação da existência de tratamento;
>
> II - acesso aos dados;
>
> III - correção de dados incompletos, inexatos ou desatualizados;
>
> IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
>
> V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
>
> VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
>
> VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
>
> VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
>
> IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.
>
> § 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.
>
> § 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.
>
> § 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.
>
> § 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:
>
> I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou
>
> II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.
>
> § 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.

> § 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional.
>
> § 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.
>
> § 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor.

Tais direitos traduzem na prática os princípios da transparência, da necessidade, da qualidade dos dados e do livre acesso, conforme já abordado anteriormente, sendo possível atestar a relação entre os três alicerces da LGPD – (i) os princípios; (ii) as hipóteses de tratamento de dados pessoais; e (iii) os direitos dos titulares –, de forma garantir o fiel cumprimento da lei.

Os elementos basilares da LGPD mencionados no parágrafo anterior guardam muita semelhança com outros regulamentos mundo afora, em especial com a GDPR, que inspirou a redação da Lei nº 13.709/2018.

Como parte do terceiro capítulo do presente trabalho, buscar-se-á analisar a relação entre a lei brasileira e o regulamento europeu para, após, entender como a aplicação da GDPR pode servir de base para o preenchimento de algumas lacunas encontradas na LGPD, bem como para a fiscalização e aplicação de penalidades pela ANPD.

2. A *COMMODITY* DOS DADOS PESSOAIS SOB A ÓTICA TRABALHISTA

Nas últimas duas décadas observou-se um avanço tecnológico acentuado, desde o salto da internet discada para o *wifi*, até a mudança de celulares antigos para os *smartphones* modernos.

Todas essas mudanças foram absorvidas pelo mundo corporativo, sendo certo que, com a digitalização tomando espaço nas relações de trabalho, as telas assumiram papel importante, substituindo, muitas vezes, documentos físicos.

Ou seja, os principais arquivos de empresas, instituições e organizações não concentram-se mais em – ou pelo menos não limitam-se mais às – vias físicas, estando armazenados principalmente em computadores, notebooks, ou até mesmo em sistemas de nuvens.

Com isso, certamente tornou-se muito mais fácil a transmissão de informações. No âmbito corporativo, tal digitalização proporciona maior facilidade para o gerenciamento do banco de dados das empresas, sejam eles comerciais ou informações pessoais dos empregados, colaboradores, e até mesmo clientes.

Tal avanço, junto à crescente valorização de dados, comina na importância da implemetação de mecanismos de segurança e prevenção contra vazamentos. Acerca da ascensão dos dados como commodities valiosas, Vólia Bonfim Cassar e Iuri Pinheiro (2022, p. 52) asseveram que

> os dados, cada vez mais, são processados e valorados economicamente, sendo considerados o principal insumo da sociedade contemporânea e equiparados ao petróleo de outros tempos. Por isso mesmo, afirma-se que a economia é dirigida por dados (*data driven economy)*.

Assim, os escândalos de vazamento de dados que ganharam destaque midiático nos últimos anos – a exemplo do caso da *Cambridge Analytica*[21] – impulsionaram as discussões acerca da necessidade de se criar uma lei geral para sua proteção no Brasil, combinados aos demais fatores econômicos que contribuíram para a edição da LGPD, conforme abordado na introdução do presente trabalho.

[21] O escândalo da Cambridge Analytica – empresa cujo principal objeto social é a mineração e tratamento de dados – veio à tona em março de 2018, quando revelou-se, através de investigações jornalísticas, que a empresa havia coletado dados pessoais de milhões de usuários da rede social Facebook de forma ilícita e vendido tais dados de forma a influenciar o resultado das eleições presidenciais estadunidenses de 2016. – Fornasier, M. de O., & Beck, C. (2020). CAMBRIDGE ANALYTICA: ESCÂNDALO, LEGADO E POSSÍVEIS FUTUROS PARA A DEMOCRACIA. Revista Direito Em Debate, 29(53), 182–195. Disponível em: https://doi.org/10.21527/2176-6622.2020.53.182-195. Acesso em: 14 de maio de 2022.

Devido ao número massivo de dados pessoais que as empresas tratam de seus empregados e colaboradores, a perspectiva da Lei Geral de Proteção de Dados Pessoais como um direito trabalhista merece destaque.

Nas palavras de Verissa Coelho Cabral Pieroni (PIERONI, 2022, p. 36, apud DONEDA, 2006, p. 152),

> o dado é o estado primitivo da informação, pois não é algo *per se* que acresce conhecimento. Dados são simplesmente fatos brutos que, quando processados e organizados, convertem-se em algo inteligível, podendo ser deles extraída uma informação.

Assim, sob a ótica das relações de trabalho, o empregador detêm um verdadeiro arsenal de informações pessoais de seus empregados e colaboradores, que agora devem ser tratadas observando-se os princípios e limites estabelecidos na Lei Geral de Proteção de Dados Pessoais.

Tais dados, incluindo dados pessoais sensíveis[22], são processados pelo empregador diariamente para diversas finalidades, e podem encaixar-se em várias hipóteses legais dentre as listadas nos incisos dos artigos 7º e 11 da LGPD, que serão abordadas em maiores detalhes em um capítulo específico deste trabalho.

Como narrado acima, é possível afirmar que a proteção de dados pessoais integra o rol de direitos da personalidade. A Lei nº 13.709/2018 traz, em seu artigo 2º[23], o livre desenvolvimento da personalidade como um dos fundamentos da lei.

A fim de protegê-lo, a LGPD garante ao titular o direito à exatidão, clareza, relevância e atualização de seus dados pessoais.[24] Dessa forma, é possível que o titular mantenha seus dados sempre atualizados e fiéis à realidade, para que a finalidade do tratamento informado pelo controlador seja atingida em sua plenitude.

---

[22] De acordo com a definição dada pela LGPD, dado pessoal sensível é "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".

[23] "Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
(...)
VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

[24] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
(...)
V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;"

Tal garantia ganha especial importância no âmbito trabalhista, na medida em que é bastante comum que os departamentos de recursos humanos coordenem testes de perfis profissionais e psicotécnicos em seus processos de recrutamento e utilizem essas informações também em processos internos decisórios.

Nesse sentido, ao realizar um planejamento estratégico ou em discussões sobre planos de carreira, os profissionais de recursos humanos muitas vezes consideram o perfil dos candidatos e/ou empregados e colaboradores para analisar a compatibilidade entre suas características e uma vaga ou posição dentro da empresa.

Sob tal perspectiva, os dados pessoais de candidatos, empregados e colaboradores são verdadeiras commodities para as empresas, adequando os perfis profissionais às melhores expectativas da organização em relação aos seus cargos ou projetos.

Apesar do direito do titular à garantia do princípio da qualidade de seus dados, é certo que a LGPD protege também os segredos comerciais das empresas.[25] Assim, é possível que para o planejamento estratégico e desenvolvimento de planos de carreira mencionados nos parágrafos anteriores, as empresas se utilizem da base legal do legítimo interesse para o tratamento de dados pessoais e reservem-se o direito de confidencialidade, observando os segredos comerciais da organização.

Nada obstante, é importante que as empresas garantam aos titulares o direito de manter seus dados pessoais atualizados, a fim mesmo de otimizar tais avaliações, na medida em que os dados serão tratados em sua melhor qualidade.

Para tanto, é essencial que as companhias observem as disposições da LGPD, em especial a contida em seu artigo 49, que determina que "os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares."

Como se vê, o verbo utilizado em tal previsão remete a uma obrigação, e não somente a uma recomendação. No entanto, para atender aos requisitos elencados na referida norma não entende-se mandatório que as empresas possuam um programa de governança em proteção de

[25] Em diversos dispositivos da Lei nº 13.709/2018 encontra-se o trecho "observados os segredos comercial e industrial."

dados estruturado em políticas e procedimentos formalizados, embora o artigo 50 da LGPD o recomende:

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Importante atentar-se ao fato de que a adoção de políticas de boas práticas e governança e de mecanismos e procedimentos internos eficazes para o tratamento de dados seguro será considerada pela ANPD quando da aplicação de sanções, como denota-se pela leitura dos incisos VIII e IX, do § 1º, do artigo 52 da LGPD:

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
> (...)
> § 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:
> (...)
> VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
> IX - a adoção de política de boas práticas e governança;

Ademais, a implementação de um programa de governança em proteção de dados eficaz será capaz de ampliar a garantia aos empregados do exercício de seus direitos como titular de dados, posto que os processos para tal exercício estarão devidamente regulados pelas políticas e procedimentos internos da organização.

Assim, resta clara a necessidade de trazer a LGPD para o âmbito das relações de trabalho, e buscar interpretá-la também como um direito trabalhista.

Para Nicolau Olivieri (2019, p. 3), “o tratamento de dados no âmbito do contrato de trabalho é, na grande maioria das vezes, a expressão de um direito do empregado e, portanto, o tratamento de dados no contexto laboral é, via de regra, feito em favor do empregado, e na defesa dos seus interesses”.

Nesse sentido, o tratamento de dados é inerente ao contrato de trabalho, e o empregador não o faz, em regra, buscando vantagens econômicas, como observa-se nas relações consumeristas, mas sim por obrigação.

No entanto, ainda que muitas vezes o empregador não tenha escolha em relação ao processamento de informações pessoais de seus empregados e colaboradores, tal fato não afasta a aplicabilidade da LGPD, que busca regular, inclusive, os tratamentos nas hipóteses de cumprimento de obrigação legal ou regulatória ou execução de contrato.

A valorização econômica dos dados impulsionou a importância de se ter uma tutela normativa de proteção das informações pessoais dos indivíduos. Como asseveram Tarcísio Teixeira e Ruth Maria Armelin (2019, p. 26), "os dados pessoais são considerados o novo petróleo da sociedade informacional, a base de um gigantesco mercado, já que através deles é possível identificar perfis de consumo, potencialidade de mercado, além de inúmeras outras possibilidades, altamente lucrativas."

Apesar de muito se falar em proteção dos dados, Laura Schertel Mendes (2014, p. 32) chama atenção para o fato de que o que se busca resguardar com a edição de leis de proteção de dados não é o dado em si, mas sim o indivíduo – o titular –, que pode sofrer algum tipo de violação à sua privacidade caso os limites agora impostos pela LGPD não sejam observados.

Nesse sentido, e considerando a proteção à privacidade do titular, o assunto ganha ainda mais contornos quando trazido para o âmbito das relações de trabalho. Isso porque muito se discute sobre os limites da privacidade do empregado quando do uso, por exemplo, das dependências e dispositivos fornecidos pelo empregador.

Essa discussão ganhou maior destaque durante a pandemia de Covid-19, quando muitas pessoas migraram para o trabalho em casa (home office), com a utilização doméstica de dispositivos fornecidos pela empregadora (notebooks, computadores, celulares, etc.).

Com isso, tornou-se cada vez mais difícil separar a vida pessoal da vida profissional, o que acabou por contribuir para que muitos empregados utilizássem os dispositivos da empregadora para fins pessoais.

Dessa forma, é sempre importante analisar caso a caso qual expectativa de privacidade o titular – *in casu*, empregados e colaboradores – pode ter sobre determinado dado. Se, por exemplo, tratar-se de um e-mail enviado de uma conta exclusivamente pessoal, a expectativa de privacidade é maior do que se o e-mail tivesse sido enviado da conta corporativa. Ainda

assim, uma análise pontual seria necessária para avaliar se o poder de monitoramento da empresa alcançaria tal dado sem violar o direito à privacidade do titular.

Nessa linha, não obstante a LGPD não ter surgido como uma lei trabalhista, como demonstrado anteriormente, sua aplicação no direito do trabalho se dará, via de regra, em favor do empregado, que tem seus dados tratados pelo empregador de forma a viabilizar o contrato de trabalho.

No entanto, ainda existem muitas lacunas e dúvidas quanto à aplicabilidade, na prática, da Lei nº 13.709/2018 nas relações de trabalho, e o que pode-se usar hoje como referencial são posicionamentos doutrinários e a atuação das autoridades de proteção de dados dos países sujeitos ao regulamento europeu de proteção de dados.

3. BREVE HISTÓRICO DA PRIVACIDADE E PROTEÇÃO DE DADOS NOS ESTADOS UNIDOS, NA EUROPA, E NO BRASIL

Como adiantado nos capítulos anteriores, o tema da proteção de dados pessoais não surgiu da noite para o dia no Brasil, tampouco em outros lugares ao redor do mundo, visto que trata-se de um instituto que vem sendo construído e consolidado desde pelo menos 1890 em alguns países.

Ademais, ainda que haja muitas similaridades na tutela da matéria ao redor do globo, é possível observar alguns pontos de divergência, tanto na forma, quanto nos assuntos regulados. Isso pode ser explicado por alguns fatores, como o sistema jurídico adotado por um determinado país, ou a maturidade que tal localidade possui em relação à regulamentação do tópico.

Assim, nos subcapítulos que seguem, busca-se ilustrar um pouco do histórico da estruturação desse tema em determinadas localidades para, após, analisar alguns pontos paralelos entre os regulamentos brasileiro e europeu.

3.1. O MODELO NORTE-AMERICANO DE PROTEÇÃO DE DADOS

Antes de adentrar no modelo europeu de proteção de dados, vale traçar um breve panorama do tema da privacidade nos Estados Unidos, representado basicamente, até então, pelo chamado “right to privacy”.

Tal elemento compõe a própria identidade do direito estadunidense e a cultura desse povo, que sempre prezou muito por sua privacidade (DONEDA, 2019, p. 215). Conforme ensina o professor David Anderson (1999, p. 139 apud DONEDA, 2019, p. 215):

> Os americanos valorizam a privacidade. Gastamos muito dinheiro e esforço para obtê-la. Na juventude, fugimos da casa de nossos pais para a privacidade de um lugar nosso. Projetamos casas para nossa privacidade. Como estudantes, preferimos apartamentos a dormitórios... Na meia-idade, colocamos nossos pais em asilos para preservar a privacidade deles e a nossa. Nós nos esforçamos para economizar dinheiro suficiente para podermos pagar, na nossa velhice, um centro de cuidados onde possamos ter a privacidade do nosso próprio apartamento. (**tradução nossa**).

O tema vem sido discutido nos Estados Unidos desde, pelo menos, 1890, quando fora publicado, em 15 de dezembro, o artigo denominado "The Right to Privacy", escrito por Samuel D. Warren e Louis D. Brandeis (1890, p. 27).

Na publicação, os autores afirmam que o direito à proteção do indivíduo é um princípio tão antigo quanto à common law, mas que é necessário, de tempos em tempos, que se definam novas formas e extensões para tal proteção.

Segundo eles, a gradação desse direito à vida culminou, à época – considerando novas invenções e métodos de negócios –, na necessidade de se dar mais um passo em direção à proteção do indivíduo, assegurando-lhe o que seria, nas palavras do juiz Tomas Cooley (1880, p. 27), o direito de ser deixado só (right to be let alone).

O referido estudo é historicamente o artigo jurídico mais citado nos Estados Unidos[26], mas, inicialmente, não fora tão bem recepcionado pelas cortes norte-americanas, a exemplo do julgamento do caso Robertson[27], no qual a existência de um right to privacy foi expressamente negada pela Corte de Apelos de Nova Iorque (DONEDA, 2019, p. 216).

No entanto, em 1905, o caso Pavesich v. New England Life Ins. Co.[28] tomou grandes repercursões por ter levado a questão à Suprema Corte da Georgia. Similarmente ao caso Robertson, nesse, discutia-se a reprodução não autorizada do retrato do Sr. Pavesich em um jornal, em contraponto a um retrato de um homem vestido com roupas rasgadas, de forma a ilustrar a prosperidade de um lado (do Sr. Pavesich), e a "miséria" do outro, em uma propaganda de uma seguradora.

No referido caso, a corte proferiu decisão contrária à anteriormente tomada pela Corte de Apelos de Nova Iorque, no caso Robertson, reconhecendo a violação ao direito à privacidade (right to privacy) mencionado no artigo de Warren e Brandeis. Tal decisão serviu como leading case, e fora, portanto, seguida por cortes de diversos estados norte-americanos (ZANINI, 2015, p. 4).

---

[26] "The most-cited law articles revisited", in: 71 Chigado-Kent Law Review 751 (1996).

[27] "Nesse caso, popularmente conhecido como o caso "Farinha da Família", a questão do direito acionável de privacidade foi pela primeira vez apresentada de forma direta. A autora buscou ressarcimento por "sua grande angústia e sofrimento no corpo e na mente", ocasionado pelos réus que imprimiam e exibiam em locais públicos uma fotografia litográfica sua, como parte de um anúncio de uma determinada farinha, e pleiteou uma liminar contra mais lesão." (**tradução nossa**). EDWARDS, Stanley. Et. al. *An actionable right of privacy? Roberson V. Rochester Folding Box Co.* ***Yale Law Journal.*** 1902, p. 2. Disponível em: https://www.jstor.org/stable/781309?seq=1. Acesso em 23 de junho de 2022.

[28] 122 Ga. 190, 50 S.E. 68 (1905).

No entanto, apesar de ter sido reconhecido jurisprudencialmente, o right to privacy não é expressamente mencionado na constituição dos Estados Unidos. De acordo com Stephen P. Mulligan e Chris D. Linebaugh (MULLIGAN; LINEBAUGH, 2019. p. 9),

> A Declaração dos Direitos dos Estados Unidos protege a privacidade individual de intrusões do governo de várias maneiras e faz muito pouco para proteger de intrusões de atores não governamentais. Algumas disposições protegem a privacidade em uma esfera relativamente estreita, como a proteção da Terceira Emenda contra o aquartelamento de soldados em residências particulares ou a proteção da Quinta Emenda contra a autoincriminação. A proteção mais geral e direta da privacidade individual está contida na Quarta Emenda, que afirma que "[o] direito do povo à segurança de suas pessoas, casas, papéis e bens, contra buscas e apreensões desarrazoadas, não será violado..." (**tradução nossa**).

Ainda, apesar de, nos anos de 1960 e 1970, a corte norte-americana ter concluído que a garantia de liberdade contida na décima quarta emenda implica a existência de um direito à privacidade geral, protegendo indivíduos de intrusões governamentais mesmo fora do escopo de buscas e apreensões, todos os direitos constitucionais envolvendo privacidade, como os "common law privacy torts" (delitos de privacidade de direito comum)[29], se concentram na divulgação pública de fatos privados, o que acaba por limitar sua potencial influência nos debates atuais de privacidade de dados. (MULLIGAN; LINEBAUGH, 2019. p. 7)

Assim, como resultado, nem a common law nem a constituição fornecem uma estrutura completa para endereçar muitas das potenciais ameaças à privacidade digital e aos dados dos indivíduos americanos. Em vez disso, os padrões de proteção de dados mais importantes vêm da lei estatutária.

Daniel J. Solove e Woodrow Hartzog (2014, p. 5) sobre a tutela do tema nos Estados Unidos, entendem que:

> A lei estatutária que regula a privacidade é difusa e discordante, e os delitos de direito comum não regulam a maioria das atividades relacionadas à privacidade. A lei de privacidade nos Estados Unidos se desenvolveu de maneira fragmentada e atualmente é uma mistura de várias proteções constitucionais, federais e estatutos estatudais, delitos, regras regulatórias e tratados. Ao contrário das leis de privacidade de muitas nações industrializadas, que protegem todos os dados pessoais de forma abrangente,

[29] "William Prosser, uma das maiores autoridades norte-americanas em *tort law*, em um artigo de 1960 intitulado simplesmente *Privacy*, fez uma importante classificação que permitiu a consolidação da *privacy* na *tort law* norte-americana. Em um estudo bastante minucioso da jurisprudência referente à privacidade, ele reconheceu a existência de um direito à privacidade, dividido em 4 modalidades e tutelado por meio de 4 *torts* ["delitos"] diferentes (...):
"1. *Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.*
2. *Public disclosure of embarrassing private facts about the plaintiff.*
3. *Publicity which places the plaintiff in a false light in public eye.*
4. *Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.*" (DONEDA, 2019, p. 236).

> a lei de privacidade nos Estados Unidos é setorial, com diferentes leis regulando diferentes indústrias e setores econômicos. (**tradução nossa**).

Assim, pode-se concluir, como será abordado a seguir, que o fato de os Estados Unidos adotarem a common law tem grande relação com a forma que a proteção de dados é tutelada no país. Diferentemente do que se vê, por exemplo, na União Europeia e no Brasil, o país norte-americano não possui uma lei geral de proteção de dados aplicável a todos os estados.

De forma a reverter isso, o governo federal norte-americano vem tentado atingir um consenso quanto à privacidade de dados. Mais recentemente, em 3 de junho de 2022, um projeto de lei bipartidário, intitulado Lei Americana de Privacidade e Proteção de Dados[30] (American Data Privacy and Protection Act), foi divulgado pelo Comitê de Energia e Comércio. O projeto de lei pretende estabelecer uma legislação abrangente de privacidade de dados, incluindo o desenvolvimento de uma estrutura nacional de privacidade de dados uniforme e um conjunto robusto de direitos de privacidade do consumidor.

Agora, o projeto de lei seguirá o processo legislativo americano e, se aprovado, representará um grande avanço no tratamento do tema no país, aproximando-o do que se espera em termos de padrões internacionais de proteção de dados.

3.2. O REGULAMENTO EUROPEU E SUA INFLUÊNCIA GLOBAL

Em um contexto de globalização cada vez mais latente, faz sentido que as leis de proteção de dados mundo afora sejam similares, considerando que os dados pessoais tornaram-se um dos principais bens comercializados ou transferidos entre empresas e instituições internacionalmente.

Nesse sentido, explica Danilo Doneda (2019, p. 186) que "há uma tendência à convergência das legislações em tema de proteção de dados, visto que as características intrínsecas da matéria não favorecem a adoção de soluções isoladas em contextos meramente nacionais".

Assim, é necessário que haja algum grau de harmonia no que diz respeito às regras aplicáveis ao tratamento de dados pessoais nos diversos países, buscando-se viabilizar negócios

[30] GAVEJIAN, Jason. Et. al. Congress Releases Draft Federal Privacy Law with Potential Traction to Pass. **The National Law Review.** 2022. Disponível em: https://www.natlawreview.com/article/congress-releases-draft-federal-privacy-law-potential-traction-to-pass#:~:text=The%20federal%20government%20has%20been,Committee%20on%20Energy%20and%20Commerce. Acesso em 24 de junho de 2022.

e transferências internacionais de forma mais eficaz e em observância às melhores práticas de mercado.

De forma geral, a Europa vem construindo uma cultura de proteção de dados desde 1970, com a criação da Lei de Proteção de Dados Pessoais do Lande de Hesse (Hessisches Datenschutzgesetz), na Alemanha Ocidental, e outras leis nacionais isoladas, como as da Suécia, França, Dinamarca, Áustria, Noruega, Luxemburgo e Islândia (DONEDA, 2019, p. 191).

Em 1973, foi publicada a Resolução (74) 29 sobre a proteção da privacidade de indivíduos vis-à-vis bancos de dados eletrônicos no setor público, adotada pelo Comitê de Ministros do Conselho da Europa, que recomendava aos estados-membros que tomassem todas as medidas necessárias para dar efeito aos princípios mencionados na Resolução, bem como que informassem à Secretaria Geral do Conselho da Europa sobre as ações tomadas nesse sentido.[31]

As recomendações contidas na Resolução mencionada no parágrafo anterior estabeleciam, entre outras coisas, que as informações armazenadas deveriam (i) ser obtidas de forma legal e por meios justos; (ii) ser precisas e mantidas atualizadas; e (iii) ser apropriadas e relevantes para o propósito para o qual foram armazenadas.

Pode-se dizer que tal Resolução continha diversos princípios hoje encontrados nas principais legislações de proteção de dados pessoais, o que demonstra que os elementos basilares do instituto de proteção de dados não sofreram tantas modificações desde que o tema começou a ser discutido.

O pontapé para a unificação legislativa sobre proteção de dados na União Europeia veio em 1981, com a Convenção 108, já mencionada nos capítulos anteriores. No entanto, somente em 1995, com a publicação da Diretiva 95/46/CE, pôde-se observar a imposição de uma obrigação comum aos estados-membros de legislarem conforme o teor da Diretiva (DONEDA, 2019, p. 196).

[31] *Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector adopted by the Committee of Ministers on 20 September 1974 at the 236th meeting of the Ministers' Deputies.* Disponível em: https://rm.coe.int/09000016807aa909. Acesso em 22 de junho de 2022.

Ainda, o Parlamento Europeu e do Conselho editou, em 12 de julho de 2002, a Diretiva 2002/58/CE[32], referente ao tratamento de dados pessoais e à proteção da privacidade no setor de comunicações eletrônicas.

Em 25 de maio de 2018, a Diretiva 95/46/CE foi revogada pela publicação da General Data Protection Regulation, com efeito em todos os estados-membros da União Europeia. A edição de um regulamento geral de proteção de dados europeu foi um grande marco para a unificação legislativa do tema na região, visto que o regulamento aplica-se diretamente em todos os estados membros, diferentemente das diretivas, que devem ser transpostas em legislações nacionais.

Apesar disso, a GDPR deixou alguns temas a serem regulamentados conforme a especificidade de cada país membro, a exemplo de seus artigos 87 – que prevê que os estados membros poderão determinar as condições específicas para tratamento de números de identificação nacional ou de qualquer outro identificador de aplicação geral – e 88 – que dispõe sobre os tratamentos no contexto da relação de emprego.

Para além do modelo europeu, há outras abordagens de tutela de proteção de dados ao redor do mundo. Conforme explica Danilo Doneda (2019, p. 186):

> A diversidade entre os sistemas de *common law* e *civil law* certamente exerceu influência no desenvolvimento de diferentes regimes de proteção de dados pessoais, sendo que uma certa resistência de países da esfera do *common law* em vincular a matéria aos direitos fundamentais ou a modelos como o da tutela da dignidade pode ser mencionada como sintomática da diferença entre enfoques.

Por outro lado, o autor explica que alguns países sob o regime de commom law contém atualmente elementos mistos em seus arcabouços jurídicos sobre proteção de dados, englobando também alguns pontos de aproximação com modelo europeu.

Assim, é possível afirmar que a GDPR é hoje o principal regulamento sobre o tema da proteção de dados do mundo, exercendo forte influência na edição de novas legislações sobre a matéria, inclusive sobre a lei brasileira.

[32] *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications.* Disponível em: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058. Acesso em 23 de junho de 2022.

No entanto, apesar de muitos pontos convergentes entre a LGPD e a GDPR, dado que o modelo europeu foi fonte de inspiração para a lei brasileira, conforme já exposto, chamam atenção alguns aspectos nos quais tais normativos divergem. É o que será explorado a seguir.

3.3. PARALELO ENTRE LGPD E GDPR

Por ter sido inspirada na GDPR, a LGPD guarda com ela muitas similaridades. No entanto, alguns pontos nos quais tais regulamentos se afastam impactam diretamente o assunto central do presente trabalho – a aplicabilidade da LGPD nas relações de trabalho.

Em primeiro lugar, a GDPR, desde sua publicação, em 2016, já determinava, através de seu artigo 51, que cada estado membro deveria estabelecer internamente uma ou mais autoridades fiscalizadoras responsáveis por monitorar a aplicação da GDPR.

Já no cenário brasileiro, a autoridade regulatória foi criada através da Medida Provisória nº 869, de 27 de dezembro de 2018, convertida na Lei nº 13.853, de 14 de agosto de 2019, que incluiu o artigo 55-A na LGPD, prevendo sua criação. No entanto, somente dois anos depois, com a edição do Decreto nº 10.474, de 26 de agosto de 2020, a ANPD teve sua estrutura regimental aprovada e publicada, sendo que apenas em novembro de 2020 a Autoridade Nacional de Proteção de Dados começou a funcionar efetivamente, com a publicação, no Diário Oficial da União, da nomeação do Diretor-Presidente do órgão.

Certamente, a diferença de prazos para estabelecimento de uma autoridade fiscalizadora impactou em como os dois regulamentos foram aplicados até então. Enquanto já se pode observar um vasto arcabouço jurisprudencial sobre o tema na Europa, no Brasil, o caminho para a aplicação da LGPD ainda encontra muitas lacunas e incertezas.

Ainda sobre o tópico, a GDPR determinou, no mesmo artigo 51 mencionado anteriormente, que as autoridades fiscalizadoras a serem estabelecidas pelos países membros deveriam ser independentes, ao passo que a ANPD é um órgão ligado à Presidência da República. De certa forma, a ausência de independência da ANPD pode gerar grandes impactos em sua autonomia para fiscalizar, inclusive, órgãos do governo e demais repartições públicas.

Outro aspecto relevante que encontra certa diferença entre as duas legislações é o da implementação de políticas de privacidade e governança. Na GDPR, tal prática é considerada obrigatória, à luz de seu artigo 24, que determina que, considerando a natureza, escopo, contexto e finalidades do tratamento, bem como os riscos de probabilidade e gravidade para os

direitos e liberdades dos titulares, o controlador deverá implementar medidas organizacionais e técnicas apropriadas para garantir e ser capaz de demonstrar que o tratamento é realizado em conformidade com a lei.

A LGPD, em contrapartida, traz, em seu artigo 50, tais medidas como uma possibilidade. Veja-se:

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, **poderão** formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. (**grifou-se**)

Dessa forma, não ficou clara a intenção do legislador quanto ao tema, ainda que tenha estabelecido, no artigo 52, § 1º, inciso IX, a adoção de política de boas práticas e governança como um dos critérios a serem avaliados quando da aplicação das sanções estipuladas na lei. Ou seja, pela pura e simples leitura da LGPD, não é possível afirmar que a implementação de políticas de privacidade e governança é obrigatória, mas sim recomendável.

Para além de outros pontos de divergência entre a LGPD e a GDPR, outro aspecto que merece destaque à luz do presente trabalho é que a GDPR, em seu artigo 88, menciona explicitamente sua aplicação às relações trabalhistas, ao determinar que cada estado membro poderá dispor sobre regras mais específicas para garantir a proteção dos direitos e liberdades relacionados ao tratamento de dados pessoais de empregados no contexto laboral. Ainda, o referido artigo traz algumas situações nas quais poderia haver tratamento de dados pessoais nas relações de trabalho, mencionando, inclusive, a possibilidade de o empregador tratar dados para promover equidade e diversidade no ambiente de trabalho.

Por outro lado, não há na LGPD qualquer menção à sua aplicação nas relações de trabalho. Esse é somente mais um dos diversos pontos nos quais a lei foi omissa, mas, ainda assim, entende-se que sua aplicação deve caminhar para o mesmo sentido estabelecido na GDPR, ao menos em relação a esse aspecto. É o que será analisado no capítulo que segue.

4. A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E AS RELAÇÕES DE TRABALHO

Após ter discorrido sobre o histórico da proteção de dados pessoais ao redor do mundo, bem como sobre a forma que este instituto vem sendo estruturado no ordenamento jurídico brasileiro, o presente estudo entra agora em seu ponto mais específico – a aplicabilidade da Lei Geral de Proteção de Dados Pessoais às relações de trabalho.

Em um primeiro momento, vale ressaltar que a LGPD é comumente associada ao direito consumerista, visto que é um dos setores nos quais mais se observou impactos com a "nova" legislação. A própria Lei nº 13.709/2018, em seu artigo 2º, inciso VI, lista a defesa do consumidor como um de seus fundamentos[33].

Ainda, o §8º do artigo 18 da referida lei traz a possibilidade de o titular dos dados exercer seu direito de peticionar em relação aos seus dados contra o controlador perante organismos de defesa do consumidor[34].

Por fim, o artigo 45 da LGPD determina que "as hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente", deixando, assim, mais que clara a aplicabilidade de suas disposições às relações consumeristas.

Por outro lado, e como mencionado no capítulo anterior, a Lei Geral de Proteção de Dados Pessoais foi omissa em relação à sua aplicabilidade às relações de trabalho, diferentemente da GDPR, que designou um artigo específico para tratar do tema e determinar que os estados membros poderiam editar normas específicas para regulamentar a matéria.

Assim, vale uma análise sobre a compatibilidade entre a LGPD e o direito do trabalho pátrio, a fim de compreender como tal aplicabilidade poderá ocorrer na prática, e quais

[33] "Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
(...)
VI - a livre iniciativa, a livre concorrência e a defesa do consumidor;"

[34] "Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
(...)
§ 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.
(...)
§ 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor."

implicações a "nova" lei geral de proteção de dados pessoais brasileira terá nas relações de trabalho.

4.1. A COMPATIBILIDADE ENTRE A LGPD E O DIREITO DO TRABALHO

Conforme adiantado nos capítulos anteriores, a Lei Geral de Proteção de Dados Pessoais não menciona expressamente sua aplicabilidade às relações de trabalho. Dessa forma, faz-se necessária uma análise de compatibilidade entre a LGPD e o direito do trabalho, para entender se o instituto da proteção de dados pessoais pode ser integrado ao direito laboral[35].

Pela simples leitura da Lei nº 13.709/2018, é possível concluir que, apesar da ausência de menção expressa sobre o tema, a referida lei também não exclui as relações trabalhistas do âmbito de sua aplicação. Logo, pode-se afirmar que a LGPD é aplicável também às atividades de tratamento de dados pessoais realizadas no âmbito das relações de trabalho[36], restando ainda algumas dúvidas sobre como tal aplicação deve ocorrer na prática.

Por sua vez, o artigo 8º[37] da Consolidação das Leis do Trabalho (CLT) é claro ao estabelecer a possibilidade de utilização de outras fontes de direito por autoridades administrativas e pela Justiça do Trabalho na resolução de lides trabalhistas. Ora, a própria CLT traz a possibilidade de aplicabilidade da LGPD nas relações de trabalho, considerando que não há no direito do trabalho regras específicas sobre o tratamento de dados pessoais.

Ainda, apesar de a Reforma Trabalhista (Lei nº 13.467/2017) ter alterado o §1º do artigo 8º da CLT para suprimir o trecho que estabelecia a necessidade de compatibilidade entre o direito comum e os princípios fundamentais do direito do trabalho para sua aplicabilidade, assevera Maurício Godinho Delgado (2018. p. 106) que

> não pode haver dúvida de que a regra subsidiária somente pode ser importante para o suprimento das lacunas nas fontes principais do campo jurídico analisado se realmente for compatível com ele, isto é, compatível com a sua estrutura normativa, com a sua lógica jurídica e com seus princípios jurídicos essenciais.

[35] Lei Geral de Proteção de Dados no Direito do Trabalho: Integração e Aplicabilidade. In: ZOGHBI, Priscila. Reflexos da LGPD no Direito e no Processo do Trabalho. São Paulo: Thomson Reuters Brasil, 2022.
[36] Leandro Sampaio Correa de Araujo (2020, p. 2) entende que o artigo 4º, inciso I, da LGPD, ao determinar que as regras para o tratamento de dados não se aplicam quando realizado por pessoa natural e não houver finalidade econômica, abre uma exceção para a aplicabilidade da LGPD às relações de trabalho doméstico, considerando a ausência de finalidade econômica da pessoa física (empregador doméstico).
[37] "Art. 8º - As autoridades administrativas e a Justiça do Trabalho, na falta de disposições legais ou contratuais, decidirão, conforme o caso, pela jurisprudência, por analogia, por eqüidade e outros princípios e normas gerais de direito, principalmente do direito do trabalho, e, ainda, de acordo com os usos e costumes, o direito comparado, mas sempre de maneira que nenhum interesse de classe ou particular prevaleça sobre o interesse público."

Nesse sentido, ao analisar o instituto do direito do trabalho e o instituto da proteção de dados pessoais, é possível reconhecer semelhanças entre seus fundamentos e princípios. O princípio da proteção – considerado o princípio basilar do direito do trabalho – encontra fortes laços com a concepção da LGPD em si.

Isso porque a Lei nº 13.709/2018 busca, em diversos dispositivos, balancear relações potencialmente desequilibradas. É o caso, por exemplo, da vedação de tratamentos de dados pessoais mediante vício de consentimento. Na verdade, esse é um dos principais temas discutidos quando da aplicação da LGPD ao direito do trabalho, considerando que as relações trabalhistas pressupõem uma hierarquia, o que por si só poderia invalidar um tratamento de dados realizado pelo empregador baseado no consentimento do empregado.

Ainda, o artigo 42 da lei traz a possibilidade de inversão do ônubs da prova no processo civil a favor do titular de dados, nos casos em que a alegação for verossível e for verificada hipossuficiência para fins de produção de provas ou quando tal produção probatória restar excessivamente onerosa ao titular.[38]

Assim, resta clara a intenção do legislador em proteger o elo mais fraco de uma relação – seja a de consumo, seja a trabalhista – no âmbito do tratamento de dados pessoais, o que está completamente alinhado com os princípios e fundamentos do direito do trabalho.

Segundo Oscar Krost (2022, p. 385),

> entre duas ou mais possibilidades de compreensão dos dispositivos da nova lei, deve-se buscar a adoção daquela que se alinhe de forma ótima aos Princípios da Proteção e suas projeções (*in dubio pro operario, aplicação da regra mais favorável e da condição mais benéfica*), da Irrenunciabilidade, da Continuidade e da Primazia da Realidade, rol meramente exemplificativo.

Não parece haver, portanto, qualquer incompatibilidade entre os dois institutos, o que torna plenamente possível a aplicabilidade da Lei Geral de Proteção de Dados Pessoais às relações de trabalho, desde que observados os princípios e fundamentos do direito laboral, e que

[38] "Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
(...)
§ 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa."

encontre-se no caso concreto necessidade de utilizar a LGPD como regra específica para preencher eventual lacuna encontrada.

4.2. A FIGURA DO CONSENTIMENTO NAS RELAÇÕES DE TRABALHO

O consentimento surge como a primeira das dez hipóteses de tratamento de dados pessoais listadas no artigo 7º da Lei nº 13.709/2018. Pode-se imaginar, a princípio, que seria a base legal mais acessível, por tratar-se de autorização dada pelo próprio titular para o tratamento de seus dados. No entanto, e muito pelo contrário, o consentimento é uma das hipóteses de tratamento de dados pessoais mais onerosas ao controlador, por diversos fatores.

Em primeiro lugar, porque pressupõe alguns requisitos específicos para ser considerado legítimo, expostos principalmente no artigo 8º da LGPD. O artigo 5º da referida lei, que traz as definições adotadas na lei, define consentimento como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".

Nesse sentido, cabe ao controlador o ônus de demonstrar que o consentimento foi dado pelo titular de forma livre e desempedida, e em conformidade com o disposto na LGPD. Ainda, caso o consentimento seja fornecido de forma escrita, deverá estar destacado de outras cláusulas contratuais, a fim de evidenciar que o titular consentiu especificamente com o tratamento para uma determinada finalidade, restando nulas as autorizações genéricas para tratamento de dados pessoais.

Ainda, é possível concluir que o consentimento é uma hipótese de tratamento frágil quando comparada às demais, considerando que pode ser revogado a qualquer momento pelo titular de dados, conforme dispõe o § 5º do artigo 8º da LGPD. Dessa forma, o controlador fica "à mercê" do titular de dados, que pode a qualquer momento interromper o tratamento ao revogar o consentimento.

No contexto laboral, a figura do consentimento é ainda mais onerosa ao controlador, considerando a hierarquia intrínseca às relações trabalhistas, o que acaba por comprometer os pressupostos necessários para que o consentimento seja considerado legítimo. Assim, o consentimento dado pelo empregado ao empregador para tratar seus dados pessoais pode ser bastante questionável, considerando que tal consentimento pode estar condicionado ao receio de contrariar o empregador.

Dessa forma, a tendência é que o empregado busque sempre agradar o empregador, a fim de conservar uma boa relação, almejando a manutenção de seu emprego ou até mesmo uma promoção. Nesse caso, entende-se que o consentimento estaria viciado, encaixando-se na hipótese do § 3º do artigo 8º da LGPD, tornando-se, portanto, inválido.

Apesar de a LGPD não prever qualquer proibição de aplicação do consentimento em contextos laborais, mesmo porque não faz qualquer menção às relações de trabalho, o considerando 43 da GDPR determina que

> 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 (...).

Nesse sentido, o Grupo de Trabalho do artigo 29 da Diretiva 95/46/CE entende que

> empregados quase nunca estão em uma posição de dar, recusar ou revogar livremente o consentimento, dada a dependência que resulta da relação empregador/empregado. Considerado o desbalanceamento de poder, empregados somente podem fornecer um consentimento livre em circunstâncias excepcionais, quando não há qualquer consequência atrelada à aceitação ou rejeição de uma oferta. (**tradução nossa**).[39]

Não obstante o acima exposto, chamar atenção para a questão da utilização do consentimento como base legal para o tratamento de dados pessoais no âmbito das relações de emprego não significa dizer que em nenhuma hipótese seria possível fazê-lo de forma adequada. Segundo Tatiana Roxo e Bianca Mollicone (2022, p. 233),

> uma forma viável de verificar a validade do consentimento dado pelos empregados é verificar se a negativa dessa manifestação seria capaz de gerar algum tipo de prejuízo ao empregado no contexto da relação de emprego. Somente aquela manfestação dada sem temor de ser prejudicado no trabalho pode ser considerada verdadeiramente livre e, portanto, válida.

Dessa forma, em um cenário em que o empregador esteja promovendo ações voluntárias, por exemplo, e o empregado deseje espontaneamente participar, o empregador poderá coletar

[39] "Employees are almost never in a position to freely give, refuse or revoke consent, given the dependency that results from the employer/employee relationship. Given the imbalance of power, employees can only give free consent in exceptional circumstances, when no consequences at all are connected to acceptance or rejection of an offer." Opinion 2/2017 on data processing at work. 2017, p. 23. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051. Acesso em 09 de julho de 2022.

os dados do empregado para tal finalidade com base em seu consentimento, sem prejuízo algum dos requisitos essenciais impostos pela LGPD.

Ainda, como o ponto central da questão é a hierarquia existente nas relações de trabalho, faz sentido que o problema assuma contornos diversos em se tratando de empregado hipersuficiente, aos quais é garantido, por força do artigo 444 da CLT, a renúncia de alguns direitos, respeitados os limites impostos pelo dispositivo (PINHEIRO; BOMFIM. 2022, p. 71).

No entanto, conforme citado anteriormente no presente trabalho, o tratamento de dados pessoais no âmbito das relações trabalhistas é, quase sempre, inerente ao próprio contrato de trabalho, não tendo o empregador outra escolha senão fazê-lo, o que faz com que haja outras hipóteses que autorizem o tratamento tanto durante o contrato de trabalho, quanto nos períodos pré e pós contratual também, conforme será explorado a seguir.

4.3. TRATAMENTO DE DADOS PESSOAIS NO PERÍODO PRÉ-CONTRATUAL

Ao contrário do que se pode pensar, o termo "tratamento de dados pessoais" não refere-se somente às operações ativas realizadas com determinada informação. Ou seja, o simples fato de um dado pessoal estar armazenado na caixa de entrada do e-mail basta para configurar tal atividade como tratamento de dados pessoais. Isso porque o artigo 5º, inciso X, da LGPD define tratamento como

> toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Nesse sentido, o simples recebimento de currículos profissionais, ainda que de forma não solicitada, constitui tratamento de dados pessoais. Nesse documento, geralmente pode-se encontrar um arsenal de dados pessoais, como nome, telefone de contato, endereço, data de nascimento, etc.

Para além do passo inicial do vínculo empregatício, processos de recrutamento comumente envolvem o tratamento de uma quantidade expressiva de dados pessoais. Não é rara a exigência de níveis absurdos de dados em diversas fases do processo seletivo, quando na

verdade a LGPD impõe o dever de observar o princípio da necessidade para que o tratamento seja considerado legal.

Por exemplo, na fase inicial do processo de recrutamento, a exigência de exames médicos não encontra respaldo na LGPD, pois não pode ser justificada como necessária àquela fase. Assim, cada fase do processo de recrutamento granulariza a quantidade e tipo de dados pessoais necessários àquela tomada de decisão, devendo o controlador observar tais limites.

O princípio da necessidade deve ser observado também em relação a quem possui acesso aos dados pessoais recebidos pela organização. Assim, é recomendável que estabeleça-se um e-mail central para recebimento de currículos, e que somente os envolvidos no processo de recrutamento tenham acesso a tais informações.

Ademais, um ponto que merece atenção é que algumas empresas optam pela adoção de processos automatizados de avaliação de currículos, por ser uma opção mais rápida e prática, o que, à luz do disposto no artigo 20 da LGPD[40], dá direito ao titular de solicitar a revisão das decisões tomadas. Assim, e conforme orientam José Filho, Aurora Dias e Luiza Brasil, "as decisões automatizadas devem seguir critérios e procedimentos bem definidos, a fim de evitar uma desclassificação discriminatória" (2022, p. 453).

Em relação à base legal recomendada nessa fase pré-contratual, o uso do consentimento pode ser questionado, considerando que a manifestação livre resta esvaziada quando o titular não possui outra escolha senão consentir com aquele tratamento – nesse caso, para o fim de sua participação no processo seletivo. Ainda, a adoção do consentimento resultaria em um ônus excessivo à organização, que teria que assegurar que cada um dos diversos candidatos consentiu de forma adequada àquela coleta de dados.

Por outro lado, é possível justificar o tratamento de dados pessoais na fase pré-contratual pelo inciso V do artigo 7º da LGPD, que traz a possibilidade do tratamento "quando necessário para a execução de contrato **ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular**, a pedido do titular dos dados" (**grifou-se**).

No entanto, parte da doutrina questiona tal base legal nesse cenário, porquanto a maioria dos candidatos inscritos não será de fato selecionado para a vaga e, portanto, contratados. Nesse sentido, também é possível a adoção do legítimo interesse como hipótese para o tratamento de

[40] "Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade."

dados pessoais na fase pré-contratual, considerando o interesse legítimo da organização em selecionar um candidato para a vaga, em harmonia com a expectativa razoável dos titulares em terem seus dados pessoais tratados para fins de participação no processo seletivo.

É o que se verifica nos casos de *background check*, através do qual o empregador realiza checagem de vínculos empregatícios anteriores, além das redes sociais e de referências profissionais do candidato, por exemplo.

Ainda na fase pré-contratual, é de suma importância que as organizações observem os princípios da LGPD, mais especificamente o princípio da necessidade, conforme mencionado anteriormente, e o da não discriminação. Nessa linha, as organizações devem ter processos de entrevistas bem definidos, de forma a analisar a necessidade de determinados questionamentos, buscando-se evitar perguntas que possam conter algum viés discriminatório, ou que violem de alguma forma a privacidade e intimidade do candidato (FILHO; DIAS; BRASIL; 2022, p. 454).

4.4. TRATAMENTO DE DADOS PESSOAIS NA FASE CONTRATUAL

Como pontuado anteriormente, o tratamento de dados pessoais no âmbito das relações trabalhistas é, quase sempre, realizado por obrigação do controlador – nesse caso, o empregador –, e não necessariamente orientado por algum interesse econômico. Assim, há duas principais hipóteses que justificam o tratamento de dados pessoais no curso de uma relação de emprego: (i) o cumprimento de obrigação legal ou regulatória; e (ii) a execução do contrato de trabalho.

Em relação à primeira hipótese mencionada acima, é o que justifica, por exemplo, o envio pelo empregador das informações do empregado ao eSocial, ou a gestão do processamento da folha de pagamento da organização. Já em relação à segunda hipótese abordada, são inúmeros os tratamentos que surgem em função da execução do contrato de trabalho.

Nesse sentido, para que o tratamento seja considerado legítimo, o controlador precisa demonstrar que ele é necessário à execução regular do contrato de trabalho, não podendo, por exemplo, justificar todo e qualquer tipo de tratamento no âmbito da relação de emprego com base nessa hipótese.

Não obstante as hipóteses acima mencionadas, o empregador poderá tratar os dados de colaboradores para o exercício regular de direitos em processo judicial, administrativo ou

arbitral. É o caso, por exemplo, do empregador que armazena cartões de pontos de seus funcionários e ex-funcionários para fins de produção de provas em processos trabalhistas.

Ademais, pode-se também justificar o tratamento de dados pessoais, inclusive dados pessoais sensíveis, dos colaboradores para fins de proteção à vida. É o que se observou com frequência durante a pandemia do vírus SARS-CoV-2 (Covid-19), com o monitoramento do estado de saúde dos empregados e gerenciamento de contatos próximos em caso de suspeita ou infecção.

Ainda, é possível que o empregador realize o tratamento de dados pessoais com base em seu legítimo interesse, para promoção das atividades da organização, desde que respeitados os direitos e liberdades fundamentais do titular, os limites e princípios elencados na LGPD, e em harmonia com a expectativa razoável do titular sobre o tratamento de determinado dado pessoal. Como exemplo, pode-se citar o monitoramento das entradas e elevadores do estabelecimento por câmeras, de forma a garantir a segurança dos colaboradores.

Em relação ao tratamento de dados pessoais baseado no interesse legítimo do controlador, a LGPD não trouxe uma lista exaustiva de situações nas quais tal base legal poderia ser utilizada para justificar um tratamento de dados. No entanto, e conforme abordado no parágrafo anterior, a lei impõe limites claros ao uso do legítimo interesse, não sendo diferente no âmbito trabalhista.

Dessa forma, é importante que o empregador sempre pondere seu poder diretivo e as expectativas razoáveis do empregado, enquanto titular de dados, acerca do tratamento de suas informações pessoais. Nessa linha, asseveram Fabiano Zavanella e Gilberto Junior (2022, p. 299) que

> não há como se admitir que o empregador ultrapasse os limites do absolutamente necessário à garantia do perfeito funcionamento de sua atividade, na forma por ele previamente definida e constantemente organizada, no que tange à imposição do seu poder diretivo e consequente subordinação do empregado.

Ainda em relação ao legítimo interesse, uma lacuna deixada pela Lei nº 13.709 é a da realização do relatório de impacto à proteção de dados pessoais. Isso porque seu artigo 10, §3º, determina que "a autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial."

Dessa forma, a expressão "poderá" não deixa claro se tal relatório deve ser elaborado pelo controlador em absolutamente todos os casos em que o legítimo interesse figure como base legal para o tratamento, ou em uma perspectiva guiada pelo risco (por exemplo, quando verificar-se um grande volume de dados sendo tratados), ou, ainda, somente mediante solicitação da ANPD.

Durante o contrato de trabalho há também o tratamento de diversos dados pessoais sensíveis, tais como origem racial ou étnica, filiação a sindicato, e dados referentes à saúde. Nesses casos, e conforme pontuado anteriormente, as hipóteses de tratamento são ainda mais restritas, considerando o potencial discriminatório desses dados. No âmbito das relações trabalhistas, as hipóteses aplicáveis a tais tratamentos são (i) consentimento do titular; (ii) cumprimento de obrigação legal ou regulatória; (iii) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral; e (iv) proteção à vida.

Nesse sentido, é necessário que o empregador, enquanto controlador dos dados, assegure que o tratamento de dados, especialmente o de dados pessoais sensíveis, no âmbito da relação de emprego seja realizado em conformidade com os princípios da Lei Geral de Proteção de Dados Pessoais, principalmente os princípios da não-discriminação e o da necessidade. Ainda, precisa ser capaz de demonstrar tal adequação através de registro que inclua, por exemplo, (i) descrição da atividade de tratamento; (ii) os dados tratados; (iii) a finalidade do tratamento; e (iv) a base legal utilizada.

4.5. TRATAMENTO DE DADOS PESSOAIS NA FASE PÓS-CONTRATUAL

Ao contrário do que se pode pensar, atividades de tratamento de dados pessoais existentes em decorrência de uma relação de emprego não se esgotam completamente quando do término do contrato de trabalho. Isso porque, ao final da relação contratual, o empregador deve reter alguns dados pessoais de seu ex-empregado por força de cumprimento de obrigação legal ou obrigatória.

É caso, por exemplo, da Instrução Normativa PRES/INSS nº 128, de 28 de março de 2022, que em seu artigo 284, §9º[41], determina que a empresa deverá manter o Perfil Profissiográfico

[41] "Art. 284. A partir de 1º de janeiro de 2004, conforme estabelecido pela Instrução Normativa INSS/DC nº 99, de 2003, a empresa ou equiparada à empresa deverá preencher o formulário PPP de forma individualizada para seus empregados, trabalhadores avulsos e contribuintes individuais cooperados, que trabalhem expostos a agentes prejudiciais à saúde, ainda que não presentes os requisitos para fins de enquadramento de atividade especial, seja pela eficácia dos equipamentos de proteção, coletivos ou individuais, seja por não se caracterizar a permanência.

Previdenciário e a comprovação de sua entrega ao trabalhador por vinte anos. Ainda, na Lei nº 8.036/1990, consta a obrigação de guarda de documentos relativos às obrigações junto ao Fundo de Garantia por Tempo de Serviço (FGTS), referentes a todo contrato de trabalho do colaborador, pelo período de cinco anos contados do término da relação de emprego.[42]

Ainda, considerando o prazo prescricional previsto nos artigos 7º, inciso XXIX da Constituição Federal[43] e 11 da Consolidação das Leis do Trabalho[44], o empregador poderá reter dados pessoais de ex-funcionários pelo período de dois anos após o término do contrato de trabalho, sempre considerando os dados referentes aos últimos cinco anos, justificando tal tratamento com base no exercício regular de direitos em processo judicial, administrativo ou arbitral.

José Filho, Aurora Dias e Luiza Brasil chamam atenção para o armazenamento de dados relacionados a doenças ocupacionais, lembrando que o Tribunal Superior de Justiça consolidou jurisprudência no sentido de que "somente quando surgirem os sintomas e que incidirá a indenização" (2022, p. 461). Assim, a fim de garantir o direito ao contraditório e à ampla defesa, o empregador poderá arquivar tais dados.

Nesse sentido, torna-se imprescindível que o empregador, na qualidade de controlador de dados, mapeie quais informações precisam ser mantidas após o término do contrato de trabalho, seja para cumprimento de uma obrigação legal ou regulatória, ou para o exercício regular de direitos em ações judiciais, administrativas ou arbitrais.

Não obstante, enquanto houver tratamento de dados pessoais pelo empregador, ainda que seja somente o arquivamento de determinadas informações, as disposições da LGPD devem ser observadas. Assim, é importante manter registro de tais tratamentos, e garantir que o

(...)
§ 9º O PPP e a comprovação de entrega ao trabalhador disposta no inciso I do § 4º deverão ser mantidos na empresa por 20 (vinte) anos."

[42] "Art. 23-A. A notificação do empregador relativa aos débitos com o FGTS, o início de procedimento administrativo ou a medida de fiscalização interrompem o prazo prescricional.
(...)
§ 3º Todos os documentos relativos às obrigações perante o FGTS, referentes a todo o contrato de trabalho de cada trabalhador, devem ser mantidos à disposição da fiscalização por até 5 (cinco) anos após o fim de cada contrato."

[43] "Art. 7º São direitos dos trabalhadores urbanos e rurais, além de outros que visem à melhoria de sua condição social:
(...)
XXIX - ação, quanto aos créditos resultantes das relações de trabalho, com prazo prescricional de cinco anos para os trabalhadores urbanos e rurais, até o limite de dois anos após a extinção do contrato de trabalho;"

[44] "Art. 11. A pretensão quanto a créditos resultantes das relações de trabalho prescreve em cinco anos para os trabalhadores urbanos e rurais, até o limite de dois anos após a extinção do contrato de trabalho."

princípio da necessidade seja respeitado, tanto em relação à quantidade de dados assim retidos, quanto às pessoas autorizadas a acessá-los.

De forma geral, independentemente da fase contratual em que ocorra o tratamento de dados, para fins de garantir a aderência da organização à LGPD é imprescindível que a devida transparência em relação ao tratamento de informações pessoais dos empregados seja assegurada.

Para isso, o controlador deve informar aos titulares sobre os tratamentos de seus dados, deixando claras as finalidades do tratamento e as bases legais que o justificam. Isso pode ser feito, por exemplo, através de aditivos aos contratos de trabalho, ou de políticas internas da companhia quanto ao tratamento de dados de seus funcionários e clientes, conforme aplicável.

Assim, o tratamento de dados pessoais no âmbito das relações de trabalho são não somente legais, mas vitais à própria execução do contrato de trabalho. Por outro lado, considerando o verdadeiro arsenal de dados que o empregador detém de seus empregados, é de suma importância seu comprometimento com os preceitos e princípios elencados na LGPD, de forma a garantir a preservação dos direitos e liberdades fundamentais de seus empregados enquanto titulares de dados.

5. PROTEÇÃO DE DADOS E RELAÇÕES TRABALHISTAS NA PRÁTICA

Conforme adiantado nos capítulos anteriores, a Lei Geral de Proteção de Dados Pessoais não foi exaustiva em todos os seus temas, deixando lacunas relevantes, algumas das quais já mencionadas neste trabalho. Dessa forma, a fim de se ter uma prévia de como se dará a aplicação da LGPD pela ANPD no contexto das relações de emprego, o presente trabalho reuniu alguns casos julgados pelas autoridades nacionais de proteção de dados dos países europeus sujeitos à GDPR, considerando as semelhanças entre ambas as leis. A seleção dos casos considerou a completude das informações disponíveis no site que reúne julgados das autoridades nacionais de proteção de dados pessoais da Europa – o *Enforcement Tracker*.

O primeiro caso[45] de execução da GDPR no contexto laboral trazido por este estudo versa sobre o uso de câmeras de vigilância no ambiente de trabalho. Nele, a Comissão Nacional de Proteção de Dados (CNPD) – órgão fiscalizador da GDPR em Luxemburgo – abriu uma investigação contra uma empresa de contabilidade que havia instalado câmeras de Circuito Fechado de Televisão (CFTV) para monitoramento do ambiente de trabalho.

Durante a investigação, os agentes notaram que havia quatro câmeras de CFTV instaladas em ambientes de livre circulação de empregados: uma no corredor de entrada que conduz às instalações do controlador; e as outras três espalhadas pelo escritório, sendo que uma das câmeras filmava também um relógio.

Ao final da investigação, concluiu-se que o controlador de dados deixou de observar o artigo 13 da GDPR, que trata do direito à informação ao titular, além do artigo 5.1. (c), que versa sobre o princípio da minimização quando do tratamento.

A empresa sancionada alegou que a finalidade do tratamento era a proteção de seus bens, visto que a empresa fora roubada em 2015, e que as informações sobre o tratamento, em geral, estariam sujeitas à publicidade adequada. No entanto, a CNPD frizou que as disposições do artigo 13 da GDPR constituem obrigação imposta ao controlador de fornecer todas as informações nele mencionadas. Assim, é atribuído ao controlador o dever de tomar medidas concretas que visem promover um nível de transparência à atividade de tratamento, de forma que sejam fornecidas todas as informações relevantes ao titular, ou orientação clara e objetiva ao indivíduo para que localize tais informações (como um link ou um *QR code*, por exemplo.)

[45] LUXEMBURGO. Comissão Nacional de Proteção de Dados. Decisão. 22 de junho de 2022. Disponível em: https://www.enforcementtracker.com/ETid-1306. Acesso em 09 de agosto de 2022.

Nesse contexto, não basta que o empregador informe ao empregado que o ambiente de trabalho está sendo monitorado por CFTV. Para fins de cumprimento da GDPR, e, no mesmo sentido, da LGPD, é necessário que sejam fornecidas, de forma facilitada e transparente, ao titular de dados, informações quanto à finalidade do tratamento, a identidade do controlador, seus direitos como titular, entre outras.

Em relação à minimização de dados, é importante que uma análise quanto à proporcionalidade entre o tratamento e a finalidade seja realizada, a fim de avaliar a necessidade do tratamento para se atingir o propósito pretendido. No caso em questão, o chefe de investigação destacou que

> Tal acompanhamento permanente pode criar pressão psicológica significativa para os funcionários que sentem e sabem que estão sendo observados, especialmente porque as medidas de vigilância persistiram ao longo do tempo. O fato de os trabalhadores em causa não disporem de meios para evadir-se periodicamente a esta vigilância também é suscetível de agravar esta pressão. Tal vigilância permanente é considerada desproporcional à finalidade pretendida e constitui uma invasão excessiva da esfera privada dos funcionários ocupados em seus cargos de trabalho. Nesse caso, os direitos e liberdades fundamentais dos funcionários devem prevalecer sobre os interesses perseguidos pelo empregador. (**tradução nossa**).

Ainda, em relação à câmera posicionada de forma a monitorar também um relógio, o agente acrescentou que tal tratamento também deve ser considerado desproporcional diante da finalidade pretendida pela empresa. A esse respeito, o chefe da investigação afirmou que "o objetivo do relógio é gerenciar e controlar as horas de trabalho e o tempo gasto pelos funcionários no local de trabalho. Incluir o relógio de ponto no campo de visão de uma câmera resulta em vigilância adicional desnecessária."

Em um outro caso[46], a Autoridade de Proteção de Dados de Berlim impôs uma multa a uma clínica médica que havia instalado 21 câmeras em suas dependências com a finalidade de proteger-se contra crimes e danos patrimoniais. Isso possibilitava à clínica monitorar seus funcionários e pacientes vinte e quatro horas por dia.

A base legal utilizada pela clínica para justificar o tratamento de dados pessoais foi o consentimento de seus empregados e avisos informacionais espalhados pela clínica. No entanto, a Autoridade Nacional de Proteção de Dados concluiu que o consentimento não poderia ser utilizado para legitimar o tratamento, uma vez que o consentimento voluntário na relação entre empregado e empregador é questionável. Ainda, entendeu que os avisos

[46] ALEMANHA. Autoridade de Proteção de Dados de Berlim. Decisão. 2021. Disponível em: https://www.enforcementtracker.com/ETid-1219. Acesso em 09 de agosto de 2022.

informacionais a respeito do monitoramento por vídeo não permitem concluir que pacientes, ao entrarem nas dependências monitoradas, expressavam legalmente seu consentimento.

Esse caso concretiza a ideia de que o consentimento é uma base legal frágil, principalmente quando utilizada no contexto laboral, pois além de ser revogável a qualquer momento e caber ao controlador o ônus de demonstrar que o consentimento foi obtido em conformidade com os requisitos da lei, a relação entre empregado e empregador atrai muitas dúvidas quanto à legitimidade do consentimento obtido.

Um outro processo[47], conduzido pela Autoridade de Proteção de Dados Italiana, resultou na imposição de multa a uma creche que havia enviado um e-mail às famílias das crianças matriculadas na instituição informando-os sobre a gravidez e licença maternidade de uma de suas educadoras.

A justificativa utilizada pela creche para o envio do referido e-mail foi a de evitar rumores em relação à ausência da professora, considerando o período de pandemia do vírus SARS-CoV-2 (Covid-19), com o intuito de proteger a titular dos dados. No entanto, a professora não havia consentido com a divulgação de sua gravidez e, portanto, a autoridade italiana concluiu que o tratamento de dados foi realizado de forma ilegal.

À luz desse caso, é possível concluir que a GDPR, e de igual forma a LGPD, trouxe obrigações importantes no âmbito do tratamento de dados pessoais sensíveis. Assim, a divulgação e tratamento de dados relacionados à saúde de funcionários, que antes costumavam ser compartilhados e divulgados sem maiores preocupações, tanto internamente quanto externamente (como no caso em questão), agora ganha diferentes contornos, lhe sendo atribuída proteção especial, por tratar-se de dado pessoal sensível.

Outro processo,[48] também conduzido pela Autoridade de Proteção de Dados Italiana, culminou na imposição de multa ao Departamento de Saúde Pública de Nápoles, que havia publicado uma nota em seu *website* contendo dados pessoais e informações sobre um procedimento disciplinar aplicado contra um funcionário.

Segundo as investigações, o controlador acreditava que a publicação de tais informações era legal, uma vez que o titular de dados havia divulgado-as à imprensa, que, por sua vez, publicou uma reportagem sobre o caso. No entanto, a autoridade italiana concluiu que

[47] ITÁLIA. Autoridade de Proteção de Dados Italiana. Decisão. 28 de abril de 2022. Disponível em: https://www.enforcementtracker.com/ETid-1193. Acesso em 09 de agosto de 2022.
[48] ITÁLIA. Autoridade de Proteção de Dados Italiana. Decisão. 13 de janeiro de 2022. Disponível em: https://www.enforcementtracker.com/ETid-1075. Acesso em 09 de agosto de 2022.

o controlador ainda assim precisaria de uma base legal para a publicação em seu *website*, independentemente de a informação ter sido publicada em outro meio de comunicação.

Esse caso parece esclarecer uma questão comumente levantada: a diferença entre dados pessoais e informações confidenciais. Não é raro que se pense que o fato de uma informação ser pública afasta a aplicabilidade das leis de proteção de dados. No entanto, a GDPR aplica-se independentemente de o dado ser disponibilizado publicamente ou não. A LGPD, no mesmo sentido, em seu artigo 7º, § 3º, estabelece que "o tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização."

Uma outra investigação[49], conduzida pela Autoridade de Proteção de Dados de Hamburgo, resultou na imposição de multa a uma empresa de moda que operava um centro de serviços em Nuremberg. Lá, desde pelo menos 2014, circunstâncias da vida pessoal de alguns empregados eram amplamente gravadas e armazenadas nos arquivos da empresa.

Como um exemplo, a empresa conduzia uma conversa de boas vindas após os funcionários retornarem de férias ou de dispensas médicas, e as informações coletadas nesse contexto, incluindo informações sobre os sintomas da doença e diagnósticos, eram gravadas e armazenadas. Ainda, de acordo com a autoridade alemã que investigou o caso, alguns supervisores escutavam as conversas a fim de tomar conhecimento sobre questões pessoais dos funcionários, como problemas de família ou convicções religiosas.

No curso do inquérito, descobriu-se que as informações armazenadas nos arquivos da companhia estavam acessíveis a cerca de cinquenta gerentes da empresa, e que eram usadas, dentre outras coisas, para avaliar a performance de trabalho dos funcionários e para obter um perfil dos empregados, de forma a tomar medidas e decisões na relação de emprego.

Esse último caso demonstra claramente o uso indevido de dados pessoais, para o qual não se tem uma finalidade legítima, tampouco uma base legal que o autorize. Em paralelo, demonstra como as leis de proteção de dados devem ser utilizadas para balizar os tratamentos de dados pessoais, de forma a guiá-los com base em seus princípios, preceitos e requisitos.

Já na realidade brasileira, pelo caráter recente da estruturação da ANPD, o que se pode verificar hoje em termos de aplicabilidade da LGPD ao contexto das relações de emprego são casos majoritariamente julgados pelo judiciário brasileiro. Até o ano de 2020, a Lei nº

[49] ALEMANHA. Autoridade de Proteção de Dados de Hamburgo. Decisão. 01 de outubro de 2020. Disponível em: https://www.enforcementtracker.com/ETid-405. Acesso em 09 de agosto de 2022.

13.709/2018 havia sido citada em mais de 130 ações judiciais trabalhistas, de acordo com dados do Valor Econômico[50].

Como exemplo, em uma reclamação trabalhista[51] movida por um ex funcionário de uma empresa, que fora dispensado por justa causa fundamentada em alegada embriaguez habitual ou em serviço, o juiz da 1ª Vara de Trabalho de Dourados aludiu a LGPD ao concluir que o empregador, enquanto controlador, não informou ao titular a finalidade do tratamento de seus dados, tampouco possuía uma base legal para o tratamento.

Ainda, entendeu que o empregador deixou de observar o princípio da necessidade, porquanto a função exercida pelo empregado (auxiliar de carga e descarga) não importava na necessidade de realização do exame etílico e, ainda, considerou o fato de que o dado pessoal em questão era um dado pessoal sensível, não havendo base legal que justificasse seu tratamento naquele contexto.

Importante salientar que as provas processuais indicavam que o empregado não aparentava estar embriagado, e que o autor da reclamação trabalhista afirmou ter ingerido álcool na noite anterior, o que justificaria a quantidade identificada no exame etílico (0,078 miligramas por litro de ar).

De todo modo, a Lei nº 13.709/2018 foi utilizada no presente caso como mais um embasamento da decisão do juiz, que entendeu que a dispensa por justa causa fora nula, tendo condenado a empresa ré ao pagamento de todas as verbas rescisórias devidas. Ainda, condenou a ré ao pagamento de danos morais, fundamento no artigo 42 da LGPD, que determina que "o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo."

Um outro ponto da LGPD que vem sido constantemente levantado em reclamações trabalhistas é o uso da geolocalização de ex-empregados como meio probatório em ações em

---

[50] OLIVON, Beatriz. Trabalhadores usam a LGPD para buscar direitos na justiça. **Valor**, São Paulo, p. 1-3, 20 jan. 2021. Disponível em: https://valor.globo.com/legislacao/noticia/2021/01/20/trabalhadores-usam-a-lgpd-para-buscar-direitos-na justica.ghtml?GLBID=1deadbe0a9d3d568650ab6f89bfeefafc7132784a56396e5639714847726a43676f63365a444c6e574d725367674c6561686976716c584442414c394a7936786b573652654448674a31555f5457466f774e79466a41424e35384b726150316c39687a413841513d3d3a303a6564756172646f2e6a2e6e65746f2e32303132. Acesso em: 08 de agosto de 2022.

[51] BRASIL. Tribunal Regional do Trabalho da 24ª Região. Sentença. Proc. nº 0024177-39.2021.5.24.0021. 1ª Vara do Trabalho de Dourados. Andre Luis Nacer de Souza. 30 de novembro de 2021. Disponível em: https://pje.trt24.jus.br/pjekz/validacao/21113011311703800000019638476?instancia=1. Acesso em 08 de agosto de 2022.

que se discutem horas extras. Assim, as empresas reclamadas têm requisitado aos juízos que determinem a quebra do sigilo dos dados de geolocalização das reclamantes, a fim de comprovar que os ex-funcionários não encontravam-se nas dependências da empresa nos momentos em que alegavam estar fazendo horas extras.

No entanto, ainda que por força do artigo 818, § 1º, da CLT caiba ao reclamante o ônus da prova em relação à realização, ou não, de horas extras, é importante avaliar se tal meio probatório observa todos os princípios e disposições da Lei nº 13.709/2018 – lei específica que deve prevalecer no caso concreto.

Caso a quebra de sigilo seja determinada pelo juízo, é necessário garantir que a coleta de dados pessoais seja restrita ao estritamente essencial para a comprovação das alegações do reclamante na ação judicial, em consoância com o princípio da necessidade, um dos pilares da LGPD.

Sobre a discussão, o advogado trabalhista Fernando Miranda (2022, p. 2), em trecho do artigo publicado pelo Jota Info, explica que se o reclamante alega estar nas dependências da empresa em um determinado horário, "a informação protegida pela privacidade – o local, horário e dias – já foi revelada no processo pelo próprio titular", não havendo o que se falar em privacidade em relação a tais dados.

No entanto, Bruno Bioni (2022, p. 3), no mesmo artigo, expôs que

> Evidentemente, os direitos à privacidade e à proteção de dados pessoais não são absolutos. Mas a relativização é desproporcional quando o tratamento das informações é feito para provar algo que seria possível por outros meios, de modo menos invasivo e com mais confiança, conforme o dever de controle de jornada da empresa.

De toda forma, não parece haver consenso, nem na doutrina, nem na jurisprudência, sobre a questão. Desse modo, será necessário avaliar no caso concreto se há outros meios capazes de produzir a prova pretendida e, em última instância, se a quebra de sigilo for determinada, tal tratamento de dados deve observar os estritos ditames da LGPD. Não obstante, é possível que a ANPD se pronuncie futuramente sobre o ponto, trazendo mais segurança jurídica para a discussão.

Como a Autoridade Nacional de Proteção de Dados ainda não regulamentou a metodologia para aplicação de multas, mesmo após quase dois anos estruturada, não há ainda registros de

sanções aplicadas pelo órgão, tampouco de processos conduzidos por ela relacionados ao tratamento de dados pessoais no contexto laboral.

No entanto, os processos movidos pelas autoridades nacionais de proteção de dados dos países europeus sujeitos à GDPR, bem como a utilização da LGPD em julgamentos de reclamações trabalhistas no judiciário brasileiro, já servem como um bom parâmetro para entender os caminhos que a ANPD poderá seguir quando da aplicação da Lei nº 13.709/2018 às relações trabalhistas.

CONCLUSÃO

De forma geral, a Lei nº 13.709/2018 não inaugurou o diploma da privacidade e proteção de dados no legislativo brasileiro. Antes dela, o instituto era regulado em legislações esparsas e não específicas sobre o assunto, como o Marco Civil da Internet, o Código Civil e a própria Constituição Federal. Apesar disso, pode-se afirmar que a Lei Geral de Proteção de Dados Pessoais abriu caminhos para maior conscientização da população brasileira sobre a importância do tema.

Se antes o fornecimento de dados pessoais em excesso para o exercício das atividades mais comuns do dia a dia era realizado sem muita estranheza, hoje, com a chegada da LGPD e a discussão frequente do tema, o cidadão brasileiro possui respaldo legal para questionar esse tipo de solicitação em estabelecimentos comerciais.

Todavia, quando encaramos a figura do titular de dados também como empregado, a autonomia para reinvindicar seus direitos à luz da LGPD é naturalmente mitigada em decorrência da hierarquia intrínseca às relações de trabalho.

Por isso, a interpretação da Lei nº 13.709/2018 no âmbito das relações trabalhistas mostra-se de suma importância, de modo a garantir que esse direito – agora fundamental, por força da inclusão do inciso LXXIX ao artigo 5º da Constituição Federal – possa ser exercido pelos titulares de dados em todas as esferas de suas vidas, inclusive na esfera trabalhista.

Como a LGPD não trouxe nenhum dispositivo específico sobre sua aplicabilidade às relações entre empregados e empregadores, alguns pontos de discussão sobre essa congruência aguardam maiores desdobramentos da execução da lei pela Autoridade Nacional de Proteção de Dados, bem como da atuação do judiciário brasileiro em ações trabalhistas que envolvam o tema.

Até o momento, os pontos em debate sobre a aplicação da Lei nº 13.709/2018 ao Direito do Trabalho estão bastante restritos à esfera doutrinária, sem maiores demonstrações de sua aplicabilidade na prática. No entanto, e em decorrência das semelhanças entre as leis de proteção de dados brasileira e europeia, pode-se extrair as expectativas em relação à aplicação da LGPD pela ANPD e pelo judiciário brasileiro da atuação das autoridades nacionais de proteção de dados dos países europeus sujeitos à GDPR.

Nesse sentido, pontos como a utilização do consentimento como base legal para o tratamento de dados pessoais de empregados e a necessidade de promoção da transparência aos

funcionários acerca das atividades de tratamento de seus dados devem receber especial atenção das empresas e organizações desde logo, considerando o que já se pode observar da aplicação da GDPR ao contexto laboral e das discussões doutrinárias sobre o assunto.

Ademais, a Agenda Regulatória da ANPD[52] para 2021 e 2022 propõe a regulamentação de pontos-chaves da Lei nº 13.709/2018, que serão essenciais para a compreensão do *modus operandi* da autoridade. Um desses pontos é a definição de metodologias que balisarão o cálculo do valor-base das sanções e multas impostas, com base no artigo 52 e seguintes da LGPD.

Como demonstrado ao longo do presente trabalho, apesar de impor novas obrigações às empresas e organizações enquanto controladoras dos dados de seus empregados e colaboradores, a Lei nº 13.709/2018 não surgiu com o intuito de impedir todo e qualquer tipo de tratamento de dados pessoais, mesmo porque isso impossibilitaria a própria existência das relações de emprego, que pressupõem um grande fluxo de informações no âmbito do contrato de trabalho.

Pelo contrário, a LGPD busca limitar as atividades de tratamento ao estrito necessário para cumprimento de uma determinada finalidade, e em observância aos princípios e preceitos impostos por ela. Assim, e em linha com os pontos levantados neste trabalho, é importante que as empresas tenham mapeadas todas as operações de tratamento de dados pessoais existentes em suas organizações para garantir que estejam de acordo com a Lei Geral de Proteção de Dados Pessoais, eliminando atividades desnecessárias.

De igual modo, é de suma importância que as empresas e organizações considerem os pontos específicos de aplicabilidade da LGPD às relações de trabalho quando do tratamento de dados de seus empregados e colaboradores, de forma a assegurar que seus direitos enquanto titulares estejam devidamente resguardados pela companhia.

Não obstante o longo caminho pela frente no processo de aculturamento da população em geral e também das organizações em relação à proteção de dados, além da estruturação incipiente da Autoridade Nacional de Proteção de Dados, é inegável que a edição de uma lei geral de proteção de dados pessoais trouxe avanços significativos para os cidadãos e para o mercado brasileiro.

[52] Agenda Regulatória da Autoridade Nacional de Proteção de Dados (ANPD). Disponível em: https://www.in.gov.br/en/web/dou/-portaria-n-11-de-27-de-janeiro-de-2021-301143313. Acesso em 07 de agosto de 2022.

Com ela, o Brasil dá um passo a frente em direção ao seu reconhecimento como um país que assegura um nível adequado de proteção de dados pessoais, bem como às garantias e direitos fundamentais dos indivíduos enquanto titulares de dados – um dos requisitos da GDPR para compartilhamento internacional de dados.

Por fim, em termos de compreensão da Lei Geral de Proteção de Dados Pessoais como um direito trabalhista, é possível concluir que ela deverá ser utilizada como lei específica, conforme aplicável, de modo a preencher lacunas eventualmente observadas no caso concreto, ao passo que o Direito do Trabalho também será capaz de esclarecer eventuais pontos nebulosos de interpretação da LGPD, trazendo elementos específicos intrínsecos às relações trabalhistas, de forma a orientar a aplicação da Lei nº 13.709/2018 nesse âmbito.

REFERÊNCIAS

ANDERSON, David. The failure of American privacy law. Basil Markensinis (org). Protecting Privacy. **Oxford: Oxford University Press**. 1999, p. 139.

BEZERRA, Maria. **Autoridade Nacional de Proteção de Dados Pessoais:** a importância do modelo institucional independente para a efetividade da lei. Caderno Virtual, [s. l.], v. 2, ed. 44, 2019. 95 p. Disponível em: https://www.portaldeperiodicos.idp.edu.br/cadernovirtual/article/view/3828/1660. Acesso em: 10 jul. 2020.

BIONI, Bruno. **Proteção de dados pessoais:** a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2021.

BRASIL. Senado Federal. Relatório Legislativo SF/18341.29177-00, de 29 de junho de 2018. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7751566&ts=1534796215492&disposition=inline&ts=1534796215492. Acesso em 27 de junho de 2022.

CONI, Vicente; FILHO, Rodolfo. A Lei Geral de Proteção de Dados e seus reflexos nas relações jurídicas trabalhistas. *In*: MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André. **Reflexos da LGPD no Direito e no Processo do Trabalho.** 2. ed. São Paulo: Thomson Reuters Brasil, 2022. P. 87-138.

DELGADO, Maurício; DELGADO, Gabriela. **A reforma trabalhista no Brasil: com os comentários à Lei n. 13.467/2017.** São Paulo: LTr, 2018. p 106.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** 2. ed. São Paulo: Thomson Reuters Brasil, 2019. 352 p.

FILHO, José Claudio; DIAS, Aurora; BRASIL, Luiza. Lei Geral de Proteção de Dados: obtenção de dados do trabalhador e limitação de uso. *In*: MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André. **Reflexos da LGPD no Direito e no Processo do Trabalho.** 2. ed. São Paulo: Thomson Reuters Brasil, 2022. P. 452-463.

KROST, Oscar. Prometeu acorrentado, LGPD e o Direito do Trabalho. *In*: MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André. **Reflexos da LGPD no Direito e no Processo do Trabalho.** 2. ed. São Paulo: Thomson Reuters Brasil, 2022. P. 380-388.

MAIA, Daniel. As hipóteses autorizativas de tratamento de dados pessoais nas relações de trabalho sob a ótica da LGPD e do GDPR. *In*: MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André. **Reflexos da LGPD no Direito e no Processo do Trabalho.** 2. ed. São Paulo: Thomson Reuters Brasil, 2022. P. 215-239.

MENDES, Laura. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental.** São Paulo: Saraiva, 2014, 246 p.

MULHOLLAND, Caitlin; FRAJHOF, Isabella. Prefácio. *In*: MULHOLLAND, Caitlin. **A LGPD e o novo marco normativo no Brasil.** 1. ed. Porto Alegre: Arquipélago, 2020. P. 11-14.

MULLIGAN, Stephen; LINEBAUGH, Chris. **Data Protection Law: An Overview.** Congressional Research Service. 2019, 79 p. Disponível em: https://crsreports.congress.gov/product/pdf/R/R45631. Acesso em 24 de junho de 2022.

OLIVIERI, Nicolau. **LGPD e sua necessária adequação às relações de trabalho**. Jota Info. Brasil: 2019, 6 p. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/lgpd-e-sua-necessaria-adequacao-as-relacoes-de-trabalho-28092019. Acesso em 25 de junho de 2022.

PAIVA, Letícia. **Juízes quebram sigilo de geolocalização de trabalhadores para checar horas extras.** Jota Info, Brasil, p. 1-8, 11 ago. 2022. Disponível em: https://www.jota.info/especiais/juizes-quebram-sigilo-de-geolocalizacao-de-trabalhadores-para-checar-horas-extras-11082022?utm_campaign=jota_info__ultimas_noticias__destaques__11082022&utm_medium=email&utm_source=RD+Station. Acesso em 13 de agosto de 2022.

PIERONI, Verissa. Noções gerais sobre proteção de dados nas relações de emprego. *In*: MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André. **Reflexos da LGPD no Direito e no Processo do Trabalho.** 2. ed. São Paulo: Thomson Reuters Brasil, 2022. P. 33-50.

PINHEIRO, Iuri; BOMFIM, Vólia. A Lei Geral de Proteção de Dados e seus impactos nas relações de trabalho. *In*: MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André. **Reflexos da LGPD no Direito e no Processo do Trabalho.** 2. ed. São Paulo: Thomson Reuters Brasil, 2022. P. 51-76.

ROXO, Tatiana; MOLLICONE, Bianca. As bases legais de tratamento de dados no ambiente de trabalho: análise da adequação entre a LGPD e a lei trabalhista. *In*: MIZIARA, Raphael;

MOLLICONE, Bianca; PESSOA, André. **Reflexos da LGPD no Direito e no Processo do Trabalho.** 2. ed. São Paulo: Thomson Reuters Brasil, 2022. P. 229-239.

SOLOVE, Daniel; HARTZOG, Woodrow. **The FTC and the New Common Law of Privacy.** Columbia Law Review. 2014, 94 p. Disponível em: https://deliverypdf.ssrn.com/delivery.php?ID=328125112117088074009003077072086029042086050028024075087068076095111110026092106074003031039025037113119011004025007093066066056040092014014022025082021091022099071040046118024006007116081073087110071010087074103019089002007121105088010127122090081&EXT=pdf&INDEX=TRUE. Acesso em 24 de junho de 2022.

TEIXEIRA, Tarcisio; ARMELIN, Ruth. **Lei Geral de Proteção de Dados Pessoais comentada artigo por artigo.** 2. ed. Brasil: Editora Jus Podivm, 2020, 12 p. Disponível em: https://www.editorajuspodivm.com.br/cdn/arquivos/9f74f5d1796969b27aa6a66908cc65cd.pdf. Acesso em 25 de junho de 2022.

WARREN, Samuel; BRANDEIS, Louis. **The right to privacy.** Harvard Law Review. 1890, 27 p. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso em 23 de junho de 2022.

ZANINI, Leonardo. **O surgimento e o desenvolvimento do *right of privacy* nos Estados Unidos.** Revista de Doutrina TRF-4. Porto Alegre: 2015, 5 p. Disponível em: https://revistadoutrina.trf4.jus.br/index.htm?https://revistadoutrina.trf4.jus.br/artigos/edicao064/Leonardo_Zanini.html. Acesso em 24 de junho de 2022.

ZAVANELLA, Fabiano; MAISTRO, Gilberto. Utilização dos dados pessoais do trabalhador e o legítimo interesse do empregador a partir do poder de direção. *In*: MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André. **Reflexos da LGPD no Direito e no Processo do Trabalho.** 2. ed. São Paulo: Thomson Reuters Brasil, 2022. P. 285-309.

ZOGHBI, Priscila. Lei Geral de Proteção de Dados no Direito do Trabalho: integração e aplicabilidade. *In*: MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André. **Reflexos da LGPD no Direito e no Processo do Trabalho.** 2. ed. São Paulo: Thomson Reuters Brasil, 2022. P. 77-86.