

**UNIVERSIDADE ESTADUAL PAULISTA “JÚLIO DE MESQUITA FILHO”
FACULDADE DE CIÊNCIAS HUMANAS E SOCIAIS**

ALUISIO RIBEIRO FERREIRA FILHO

**A LEI GERAL DE PROTEÇÃO DE DADOS E OS DIREITOS
FUNDAMENTAIS DOS TRABALHADORES**

FRANCA

2021

ALUISIO RIBEIRO FERREIRA FILHO

**A LEI GERAL DE PROTEÇÃO DE DADOS E OS DIREITOS
FUNDAMENTAIS DOS TRABALHADORES**

**Trabalho de Conclusão de Curso apresentado
ao Curso de Direito da Faculdade de Ciências
Humanas e Sociais, Universidade Estadual
Paulista “Júlio de Mesquita Filho” como parte
das exigências para obtenção do título de
Bacharel em Direito.**

**Área de concentração: Direito do Trabalho
Orientador: Prof. Dr. Victor Hugo de Almeida**

FRANCA

2021

F3831	<p>Ferreira Filho, Aluisio Ribeiro</p> <p>A Lei Geral de Proteção de Dados e os Direitos Fundamentais dos Trabalhadores / Aluisio Ribeiro Ferreira Filho. -- Franca, 2021</p> <p>111 f.</p> <p>Trabalho de conclusão de curso (Bacharelado - Direito) - Universidade Estadual Paulista (Unesp), Faculdade de Ciências Humanas e Sociais, Franca</p> <p>Orientador: Victor Hugo de Almeida</p> <p>1. Direito. 2. Direito do Trabalho. 3. Direito Digital. 4. Proteção de Dados Pessoais. 5. Direitos Fundamentais dos Trabalhadores. I.</p> <p>Título.</p>
-------	---

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca da Faculdade de Ciências Humanas e Sociais, Franca. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

ALUISIO RIBEIRO FERREIRA FILHO

**A LEI GERAL DE PROTEÇÃO DE DADOS E OS DIREITOS
FUNDAMENTAIS DOS TRABALHADORES**

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da Faculdade de Ciências Humanas e Sociais, Universidade Estadual Paulista “Júlio de Mesquita Filho” como parte das exigências para obtenção do título de Bacharel em Direito. Área de concentração: Direito do Trabalho.

BANCA EXAMINADORA

Presidente: _____
Prof. Dr. Victor Hugo de Almeida

1º Examinador: _____

2º Examinador: _____

Franca, _____ de _____ de 2021.

AGRADECIMENTOS

O presente trabalho corresponde ao fim de uma saudosa etapa de minha vida. Jornada esta que proporcionou inúmeras oportunidades para que pudesse evoluir, de maneira que não seria possível concluí-la se não tivesse me apoiado nos ombros de gigantes. Por mais clichê que a frase de Sir. Isaac Newton possa transparecer, seu conteúdo permanece verídico, de forma que tecerei algumas simples e singelas palavras para agradecer as principais personagens desse capítulo de minha história.

Primeiramente, agradeço ao meu Pai Celestial e meu São Jorge que sempre me guiaram e trouxeram boas energias e oportunidades ao meu caminho.

Agradeço àqueles que são os pilares centrais de minha vida: minha mãe Eliana e meu pai Aluisio, cujos sacrifícios possibilitaram direta ou indiretamente quase que a integralidade das oportunidades de minha vida. Pretendo honrá-los e respeitá-los sempre, de modo almejo agradecer-lhes não só com outras palavras, mas também com acontecimentos que lhes tragam muitas felicidades e orgulho.

Agradeço à minha namorada, Jennifer Ribeiro, por todo o companheirismo, paciência, momentos vividos e apoio na vida e na graduação, em especial, pelos meus textos, trabalhos e artigos por ela analisados.

Agradeço aos meus veteranos Frederico Ramos Bonfim e Túlio Tito Borges por terem me recebido e tratado sempre tão bem e guiado, da melhor maneira possível, meus primeiros passos dentro da graduação lá no ano de 2017.

Agradeço ao Felipe Scandiuzzi, por todo o convívio e companheirismo ao longo de nossos anos no apartamento 627 (nosso Congresso), dos primeiros contatos, à escolha de nosso apartamento, passando pelos cachorros raivosos, muitos momentos de crescimento até a despedida antecipada pela pandemia. Aproveito o momento para agradecer também aos demais amigos do “grupão”: Bruna Modesto, Debora Amorim, Emily Costa, Fabiana Gil, Luisa Guedes, Rayra Faria por cada momento juntos, cada companhia, pelos surtos coletivos, trabalhos, provas, petiscarias, apoios, críticas, aventuras, estrogonofes (strogo-ons) e festinhas. Orgulho fazer parte de nossa família “Rousseau”.

Agradeço também aos meus primeiros colegas de trabalho: Betina Yagi, Gustavo Maciel e Heloisa Guerra, que se tornaram grandes amigos, desde os primeiros mapeamentos de processos, nosso jeito “gestão” de ser, nossos cafés e momentos vividos.

Agradeço à Empresa Júnior EJUR Soluções Jurídicas e a todo o aprendizado e crescimento pessoal e profissional por ela proporcionado, também pela inserção no Movimento Empresa Júnior, estendendo também os cumprimentos a: Ana de Mari, Barbara Brandão, Ester Segalla, Felipe Polesel, Guilherme Morelli, Hélio Santos, Marina Diniz, Nicole Vasconcelos, Paulo Cereda, Sophia Ré, Thales Flausino.

Agradeço ao Borges, Cunha & Vaz Advogados, bem como ao Dr. José Vaz e aos membros do “Egrégio Tribunal dos Estagiários”: Álick Souza, Gabriel Bina, Luiz Andreotti, Manollo Sedano por todos os momentos e aprendizados trabalhistas.

Agradeço ao Juizado Especial Cível – Anexo UNESP, a todos os conciliadores, bem como aos escreventes Rejanie e Ernani.

Agradeço aos grupos e seus membros: GEPPIDES (Grupo de Estudos e Pesquisa em Propriedade Intelectual e Desenvolvimento Econômico-Social) e RETRAB (Núcleo de Pesquisa e Observatório Jurídico (Re)Pensando o Trabalho Contemporâneo) que marcaram minha vida acadêmica e muito me ensinaram.

Agradeço ao Professor Victor Hugo de Almeida, por todo o apoio, conselhos e correções acadêmicas durante o desenvolvimento de nossas pesquisas e parcerias em artigos publicados.

Agradeço também à PROPe - Pró Reitoria de Pesquisa pela bolsa PIBIC da iniciação científica concedida a mim por dozes meses entre 2020 e 2021, que possibilitou o desenvolvimento da pesquisa que culminou também no presente trabalho.

*“Globalização através do direito,
não através do mercado.”
Stefano Rodotà*

FERREIRA FILHO, Aluisio Ribeiro. **A Lei Geral de Proteção de Dados e os direitos fundamentais dos trabalhadores**. Orientador: Victor Hugo de Almeida. 2021. 111 f. Trabalho de Conclusão de Curso (Graduação em Direito) – Faculdade de Ciências Humanas e Sociais, Universidade Estadual Paulista “Júlio de Mesquita Filho”, Franca, 2021.

RESUMO

A proteção de dados pessoais emergiu como uma necessidade para o mundo contemporâneo globalizado. Assim, surgiram diversas legislações ao redor do mundo para regular o tema. No Brasil, é sancionada, no ano de 2018, a Lei nº 13.709/2018, mais conhecida como Lei Geral de Proteção de Dados (LGPD). Tal legislação almeja regular as operações envolvendo dados pessoais no país. Diante disso, surge o questionamento a respeito da possibilidade de aplicação da mencionada lei às relações de trabalho. Assim, o objetivo do presente é examinar as mudanças possibilitadas pela vigência da Lei Geral de Proteção de Dados nos direitos fundamentais dos trabalhadores, com enfoque sobre sua privacidade, bem como das formas de adequação do empregado privado ou público a esse cenário. Para isso, adota-se a técnica da pesquisa bibliográfica em materiais já publicados, como método de procedimento; e, como método de abordagem, adota-se o dedutivo. Conclui-se que a Lei Geral de Proteção de Dados é aplicável à relação laboral, de maneira que repercute no uso do consentimento como base legal de tratamento, bem como nos processos seletivos e análises curriculares de candidatos, inclusive adolescentes. Reflexos também são encontrados sobre a ampliação de conteúdo passível de regulação por meio das negociações coletivas, assim como também sobre a imposição de limites à utilização de dados pessoais de trabalhadores nas organizações de tendência e também na divulgação da remuneração dos empregados públicos pela Administração Pública; e, por fim, na limitação do uso de informações pessoais de trabalhadores pelo empregador, ao final de um processo seletivo ou do contrato de trabalho.

Palavras-chave: dados pessoais; Direito do Trabalho; direitos fundamentais dos trabalhadores; Lei Geral de Proteção de Dados; privacidade.

FERREIRA FILHO, Aluisio Ribeiro, **The General Data Protection Law and the employees' fundamental rights**. Advisor: Victor Hugo de Almeida. 2021. 111 f. Monograph (Bachelor in Law) – Faculty of Humanities and Social Science, Universidade Estadual Paulista “Júlio de Mesquita Filho”, Franca, 2021.

ABSTRACT

The protection of personal data has emerged as a necessity for the contemporary globalized world. Thus, several laws emerged around the world to regulate the subject. In Brazil, in 2018, Law n° 13.709/2018, better known as the General Data Protection Law (LGPD) is enacted. Such legislation aims to regulate operations involving personal data in the country. As a consequence, the question arises regarding the possibility of applying the aforementioned law to labor relations. Thus, the objective of the present is to examine the changes made possible by the Lei Geral de Proteção de Dados in the fundamental rights of employees, focusing on their privacy, as well as the ways of adequate the private or public employee to this scenario. For this, the technique of bibliographic research in previously published materials is adopted, as a method of procedure; and, as an approach method, the deductive one is adopted. It is concluded that the Lei Geral de Proteção de Dados is applicable to the labor relationship, so that it has repercussions on the use of consent as a legal basis for treatment, as well as on the selection processes and curricular analysis of candidates, including teenagers. Reflections are also found on the expansion of the content subject to regulation through collective bargaining, as well as on the imposition of limits on the use of workers' personal data in tendency organizations and also on the disclosure of public employees' remuneration by the Public Administration; and, finally, on the limitation of the use of workers' personal information by the employer, at the end of a selection process or employment contract.

Keywords: fundamental rights of the employees ; Labor Law ; Lei Geral de Proteção de Dados; personal data. privacy.

SUMÁRIO

1 INTRODUÇÃO	10
2 OBJETIVO	12
2.1 Objetivo geral	12
2.2 Objetivos Específicos	12
3 MÉTODO E MATERIAIS	13
4 OS DADOS E A PROTEÇÃO LEGAL DO DIREITO À PRIVACIDADE	14
4.1 A inserção dos dados na sociedade contemporânea	14
4.2 Os dados e a proteção do direito fundamental à privacidade	17
4.2.1 <i>Economia digital e o upgrade do direito à privacidade</i>	18
4.3 Antecedentes à proteção brasileira de dados	21
4.4 A proteção dos dados no Brasil	25
5 LEI GERAL DE PROTEÇÃO DE DADOS	29
5.1 Histórico: tramitação legislativa e o efeito dominó	29
5.2 Definições gerais e preceitos essenciais	33
5.2.1 <i>Conceitos</i>	33
5.2.2 <i>Princípios</i>	36
5.2.2.1 Boa-fé	37
5.2.2.2 A trindade da finalidade, adequação e necessidade	38
5.2.2.3 Livre acesso	42
5.2.2.4 Qualidade dos dados	43
5.2.2.5 Transparência	43
5.2.2.6 Segurança	44
5.2.2.7 Prevenção	45
5.2.2.8 Não discriminação	47
5.2.2.9 Responsabilização e prestação de contas	47
5.2.3 <i>Bases Legais de Tratamento</i>	48
6 IMPACTOS DA LGPD NO CONTEXTO LABORAL	51
6.1 LGPD e sua aplicabilidade no âmbito laboral	51
6.2 Consentimento e a proteção de dados dos trabalhadores	54
6.3 Análises curriculares e a proteção de dados	58
6.3.1 <i>Processos seletivos: currículos e o tratamento de dados</i>	58
6.3.2 <i>Estagiários e aprendizes: currículos de crianças e adolescentes</i>	62

6.4 Negociação coletiva e a LGPD	66
6.4.1 <i>Negociação coletiva e proteção de dados</i>	66
6.4.2 <i>Artigo 611-A da CLT: prevalência do negociado sobre a LGPD</i>	68
6.5 Proteção de dados dos empregados em organizações de tendência	71
6.5.1 <i>Raízes históricas e definições</i>	71
6.5.2 <i>Ideologia e o tratamento de dados sensíveis</i>	73
6.6 Proteção de dados dos empregados públicos	76
6.6.1 <i>Princípio da publicidade</i>	77
6.6.2 <i>Empregados públicos e o Direito do Trabalho</i>	79
6.6.3 <i>Da razoabilidade e proporcionalidade à necessidade na proteção de dados</i>	80
6.7 Limitação do tratamento de dados no âmbito laboral	86
6.7.1 <i>Fim do tratamento em processos seletivos e guarda de currículos</i>	87
6.7.2 <i>Término do contrato de trabalho</i>	89
7 CONCLUSÃO	94
REFERÊNCIAS	99

1 INTRODUÇÃO

O desenvolvimento das tecnologias causou os mais variados impactos na sociedade. Neste contexto, o fluxo de informações cresceu intensamente, de maneira que os dados elevaram-se a posições de suma importância dentro da sociedade e também de grande parte da economia mundial.

Ocorre que os dados pessoais, além de tornarem-se insumos capazes de auxiliar empresas e fixarem-se como mercadoria, também podem integrar conotações relativas à privacidade das pessoas naturais. Isso decorre do fato de que informações pessoais podem estar atreladas aos aspectos mais íntimos de cada indivíduo, merecendo assim proteção legal e constitucional especiais.

Por isso, inúmeras legislações passaram a regular as operações envolvendo dados pessoais. Dentre elas, cita-se a Lei Geral de Proteção de Dados (LGPD), sancionada em 2018 e com vigência iniciada em 2020. Essa legislação instituiu diversos parâmetros para que os dados fossem operacionalizados, devendo-se observar dispositivos legais e princípios.

Embora a LGPD não expresse sua aplicação na seara laboral, ela deverá ser feita como forma de garantir os direitos relativos à privacidade e personalidade do trabalhador.

Por isso, o presente trabalho se propõe a investigar quais as alterações proporcionadas pela vigência da Lei Geral de Proteção de Dados nos direitos dos trabalhadores, com enfoque inicial relacionado ao direito à privacidade. Serão examinadas, também, as mudanças e meios de adequação do empregador pessoa física e pessoa jurídica e até da Administração Pública.

A estrutura do presente trabalho contempla três tópicos. O primeiro (os dados e a proteção legal do direito à privacidade) almeja elucidar a maneira pela qual os dados pessoais foram inseridos na sociedade contemporânea, bem como a relação das informações pessoais e o direito fundamental à privacidade, de modo a apresentar como este último evoluiu e relaciona-se com a economia digital. Também se abordam os antecedentes legislativos à proteção de dados no mundo e, ainda, sobre o desenvolvimento da proteção de dados no Brasil.

No segundo item (Lei Geral de Proteção de Dados) examinam-se os aspectos relacionados à LGPD especificamente, de modo a explicitar como fora feita a tramitação legislativa que culminou na lei, bem como as suas atuais definições gerais: conceitos, princípios e bases legais de tratamento.

No que tange ao terceiro tópico (impactos da LGPD no contexto laboral), analisa-se a interseção entre a proteção de dados pessoais, direitos dos trabalhadores e deveres do

empregador, por meio do estudo de alguns aspectos, quais sejam: aplicabilidade da LGPD na seara laboral; o consentimento como base legal de tratamento de dados dos trabalhadores; análises curriculares, processos seletivos e a proteção de dados; negociações coletivas envolvendo a proteção de informações pessoais; proteção de dados nas organizações de tendência; proteção de dados dos empregados públicos; e, por fim, a limitação e o término do tratamento de dados.

2 OBJETIVO

2.1 Objetivo geral

Investigar quais as alterações proporcionadas pela vigência da Lei Geral de Proteção de Dados nos direitos dos trabalhadores, com enfoque inicial relacionado ao direito à privacidade. Também serão examinadas as mudanças e meios de adequação do empregador pessoa física e pessoa jurídica e até a Administração Pública.

2.2 Objetivos Específicos

- a) Compreender a inserção dos dados na sociedade e no mercado global contemporâneo;
- b) Delinear como se dá a relação entre proteção de dados e a defesa do direito à privacidade;
- c) Examinar a evolução legislativa mundial sobre a proteção de dados;
- d) Analisar o aperfeiçoamento da proteção de dados no Brasil;
- e) Estudar a desenvolvimento da Lei Geral de Proteção de Dados, bem como seu histórico, conceitos, princípios e bases legais de tratamento; e
- f) Elencar algumas mudanças da Lei Geral de Proteção de Dados nos direitos dos trabalhadores, deveres dos empregadores e cotidiano laboral, especificamente sobre:
 - i. Sua aplicabilidade no âmbito laboral;
 - ii. Escolha do consentimento como base legal de tratamento de dados de trabalhadores;
 - iii. Análise de currículos, processos seletivos e proteção de dados;
 - iv. Confluência entre negociação coletiva e a proteção de dados;
 - v. Tratamento de dados sensíveis nas organizações de tendência; e
 - vi. Limite temporal e a eliminação dos dados dos trabalhadores.

3 MÉTODO E MATERIAIS

Como método de procedimento, utiliza-se a técnica de pesquisa bibliográfica, visando à análise da Lei Geral de Proteção de Dados e dos direitos fundamentais dos trabalhadores e dos deveres do empregador, com enfoque maior para o direito à privacidade. Tal técnica consiste no contato direto da bibliografia já tornada pública em relação ao tema, o que propicia o exame sob nova abordagem, permitindo o reforço paralelo na análise da pesquisa e a manipulação de informações (LAKATOS; MARCONI, 2003).

Utilizam-se materiais já publicados, como, por exemplo, artigos científicos, monografias, dissertações, jurisprudência, legislação nacional e internacional, conteúdos disponibilizados em sítios eletrônicos, entre outros.

Como método de abordagem, adota-se o dedutivo, a fim de se extrair particularidades de premissas gerais relacionados ao fenômeno em estudo (FONSECA, 2009); ou seja, a partir da compreensão da Lei Geral de Proteção de Dados e dos direitos fundamentais dos trabalhadores, visa identificar seus impactos no contexto laboral, explicitando as alterações no cotidiano das empresas e até mesmo para a administração pública.

4 OS DADOS E A PROTEÇÃO LEGAL DO DIREITO À PRIVACIDADE

O avanço da globalização e das tecnologias proporcionou uma conectividade jamais antes vista pelo mundo. Aliado a isso, surgem novos modelos de negócio, bem como relações sociais inéditas e suas respectivas respostas legais. Nesse cenário, os dados passam a ter grande relevância para a economia mundial, sendo considerados como seu elemento central, haja vista que também se tornaram um ativo para as empresas, assim como também um produto a ser comercializado.

Ocorre que, possivelmente, os dados pessoais estão relacionados a um conteúdo intrínseco da pessoa natural, podendo ser parte de sua intimidade, privacidade. Diante disso, surge a necessidade de regulamentação de seu uso pelas empresas. Embora a Constituição Federal de 1988 preveja a proteção à privacidade, a mesma não está adequada às atuais imprescindibilidades de proteção de dados pessoais, necessitando atualizar-se.

Nesta conjuntura, surgem diversos meios protetivos aos dados de pessoas físicas ao redor do mundo, sendo antecedentes à proteção brasileira de dados. As primeiras legislações relacionadas à temática surgiram em torno dos anos 1960 e seguiram contornando limites às operações envolvendo informações pessoais em alguns países, com destaque para os Estados Unidos e a União Europeia.

Inserido neste contexto, convém também analisar como a proteção de dados brasileira foi formada. Inicialmente, houve um vazio de especificidade de leis ligadas ao tema, cabendo ao ordenamento jurídico já presente, a atuação na garantia da proteção de dados. Neste contexto, destaca-se a normatividade expressa no Código de Defesa do Consumidor e também do *habeas data*, sendo este previsto constitucionalmente.

4.1 A inserção dos dados na sociedade contemporânea

A economia mundial já perpassou por diversas fases, com diferentes elementos que a caracterizavam. Por exemplo, a escola mercantilista surgida na Idade Média pregava o acúmulo de riquezas através de ouro e prata, além da ampliação de monopólios comerciais via exploração de suas colônias, conforme explica Stanley Brue (2005). Por outro lado, o capitalismo industrial, datado entre os anos de 1760 e 1850, foi responsável por algumas inovações técnicas, como as relacionadas às indústrias do ferro e têxtil, além do uso das máquinas a vapor, segundo Flávio Saes e Alexandre Saes (2013).

Contudo, o estágio atual da economia mundial é amplamente influenciado pelas modificações proporcionadas pela globalização e suas tecnologias. Bruno Bioni (2021) esclarece que o desenvolvimento tecnológico propiciou o surgimento de fluxos de informações em quantidades e velocidades nunca antes presenciadas pelo mundo, ultrapassando barreiras físicas, de maneira a proporcionar tamanha importância aos dados que se tornaram elemento central do desenvolvimento das economias.

Os dados pessoais passaram a ter alto teor de importância para as empresas, haja vista que através deles podem-se mensurar os gostos de seus clientes, parceiros comerciais, até mesmo empregados. Assim, seria possível um melhor direcionamento das ações e vendas de uma empresa, com foco para atrair os gostos já identificados dos indivíduos.

A título de exemplo, pode-se citar o caso dos *cookies*. Os mesmos correspondem a arquivos que contêm informações coletadas dos usuários de internet conforme o mesmo a utiliza, de modo a salvar preferências do internauta. Assim, em um próximo uso, o site já estará adaptado aos desejos e inclinações dos usuários, seja para providenciar uma melhor navegação ou para divulgação de anúncios, instituindo a chamada “publicidade comportamental”, consoante o entendimento de Joana Silva (2020, p. 23).

Interessa ressaltar que os dados obtidos por uma empresa podem ser utilizados como insumo para suas atividades, mas também como um produto final a ser comercializado com outras pessoas jurídicas. Alice Sampaio (2017) explica o caso das empresas corretoras de dados ou *data brokers* que angariam dados públicos, governamentais e comerciais, possibilitando uma segmentação populacional de acordo com informações de interesse do comércio, como pela renda, localização, interesses, entre outros. Com essas informações coletadas, passam a vendê-las a outras empresas, que as utilizarão para atualizar base de dados, melhoria de produtos, direcionamento do marketing, entre outras finalidades.

Como forma de ilustrar melhor esse novo modelo de negócio, bem como sua força e aplicabilidade sutil no dia a dia, é válida a citação do caso da empresa varejista Target. Kashmir Hill (2012) noticia que um pai fora reclamar na sede da Target que a filha estava sendo instigada a engravidar, já que, apesar de ainda estar no colegial, recebia e-mails da varejista de cupons de fraldas e berços.

Contudo, em um futuro próximo, o pai descobriu que a filha já estava grávida e ele não sabia. Intrigante notar que, através dos dados pessoais relacionados às compras anteriormente realizadas pela moça na Target, a empresa, suas tecnologias e algoritmos puderam estabelecer um padrão de compra de uma grávida, de modo a evidenciar que a

mencionada filha, provavelmente, estava grávida, constatando isso antes mesmo da família ter conhecimento, motivo pelo qual eram enviados os cupons acima relatados pelo pai.

É relevante citar o fato de que, embora as exposições de dados pessoais sejam parte do cotidiano da sociedade, esta se estrutura de modo a dificultar a percepção desse fenômeno, já que a exposição de informações pessoais é a regra, de forma que o indivíduo vê-se coagido à exposição de seus dados pessoais como uma maneira de inserir-se na sociedade e ser nela aceito. Sobre esse fenômeno, Byung-Chul Han (2017, p. 31-32) disserta:

Na sociedade expositiva cada sujeito é seu próprio objeto-propaganda; tudo se mensura em seu valor expositivo. A sociedade exposta é uma sociedade pornográfica; tudo está voltado para fora, desvelado, despido, desnudo, exposto. O excesso de exposição transforma tudo em mercadoria que ‘está à mercê da corrosão imediata, sem qualquer mistério’. A economia capitalista submete tudo à coação expositiva, é só à encenação expositiva que gera valor, deixando de lado todo e qualquer crescimento próprio das coisas.

Outra situação que evidencia o poder dos dados pessoais e como vêm sendo utilizados pela indústria, é o dos sites de compras na internet. É comum que, após uma pesquisa em sites de vendas feita pelo computador ou celular, comece a aparecer propagandas muito semelhantes à pesquisada, ao navegar-se em uma rede social. Isso ocorre através do direcionamento proporcionado pelo cookies, acima explicados, como assevera Guilherme Tagiaroli e Rodrigo Lara (2021).

Por fim, é de vital importância uma breve explanação envolvendo os escândalos da *Cabridge Analytica*. Esta, segundo Marcelo Martins e Victor Tateoki (2019), é uma empresa britânica que desenvolve estratégias de marketing através do manuseio de informações pessoais, traçando uma espécie de publicidade direcionada e comportamental.

Martins e Tateoki (2019) defendem que essa empresa atuou de modo assertivo e decisivo nas eleições norte-americanas de 2016, nas quais Donald Trump fora eleito. Para isso, foram utilizados milhões de dados pessoais captados pela rede social *Facebook*, de modo que os eleitores teriam sido manipulados através de suas predileções observadas via mídia social. Letícia Oliveira (2021) também assegura que a atuação da *Cambridge Analytica*, feita de forma semelhante ao caso acima, foi fundamental para que o Reino Unido saísse da União Europeia, movimento que ficou conhecido como *Brexit*.

Assim, os dados tornaram-se um ativo, uma mercadoria, um mecanismo capaz de guiar as ações mercadológicas, bem como também um produto a ser comprado e vendido, podendo influenciar até mesmo eleições nacionais. Marcelo Benacchio e Renata Maciel

(2020, p. 56) denominam esta nova fase capitalista, em que os dados são sua mercancia fulcral, de “mercantilização digital”. Notável que essa inserção dos dados pessoais na sociedade contemporânea é sutil, mas também muito presente no cotidiano dos indivíduos.

4.2 Os dados e a proteção do direito fundamental à privacidade

Embora a “economia digital” e seu modelo de negócios, vide ensinamentos de Patrícia Peck Pinheiro (2021, p. 10), são dependentes dos dados, o surgimento das primeiras leis protecionistas de dados pessoais surgiram ainda por outros motivos. A autora sugere que houve uma recuperação dos compromissos das instituições para com as pessoas físicas, como na garantia dos direitos humanos fundamentais, com destaque para a privacidade, elencada desde 1948 através da Declaração Universal dos Direitos Humanos.

No que se refere ao direito fundamental à privacidade, rememora-se que o mesmo encontra-se previsto no inciso X do artigo 5º da Constituição Federal (BRASIL, 1988): “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;”

Alexandre de Moraes (2021) explica que a privacidade está atrelada à garantia da manutenção da identidade de cada indivíduo em face de quaisquer pressões sociais ou políticas. O escritor ainda elenca exemplos de defesa desse princípio fundamental através da proteção contra: intromissões em sua vida particular, doméstica, familiar; ataques à sua honra e reputação; a espionagem; ingerência na sua correspondência, dentre outros.

Em outro diapasão, José Afonso da Silva (2008, p. 206-207) defende que a privacidade possibilita o controle do indivíduo sobre seus próprios dados ou informações. O autor ainda comenta que, caso pretenda, a pessoa pode comunicá-las, através do local e condições por ela desejadas. Com amparo na doutrina norte-americana, compara-se o direito à privacidade ao “direito de ser deixado tranquilo, em paz, só: *Right to be alone*”. Ainda identifica tal direito a outros previstos constitucionalmente: à inviolabilidade de domicílio, sigilo profissional e de correspondência.

Em torno do apresentado, é possível configurar o direito à privacidade como a garantia de proteção e controle do indivíduo sobre suas informações pessoais e íntimas, tanto em sentido amplo como em sentido estrito. Assim, o domínio sobre seus dados deve ser feito, exclusivamente, pela pessoa a quem eles se referem, não havendo interferências, a princípio, nem mesmo do Estado.

4.2.1 Economia digital e o upgrade do direito à privacidade

Resta cristalino que a economia digital passou a ter os dados como elemento central de sua desenvoltura. Destarte, por serem relacionadas a indivíduos certos, as informações podem apresentar caráter de intimidade, sendo de tal modo intrínseco às pessoas que estão inseridas no seu direito à privacidade, merecendo também proteção e sigilo especial.

Alexandre de Moraes (2021) salienta que a garantia de sigilo e proteção de dados é conquista recente proporcionada pela Constituição Federal de 1988, através dos direitos fundamentais da vida privada e intimidade, elencados pelo inciso X do artigo 5º. Estes últimos são explicados pelo autor como presunções da defesa da privacidade, assegurando identidade à pessoa.

Assim, para que a privacidade da pessoa natural seja garantida, a mesma também deverá ter controle sobre suas informações pessoais. Para isso, o direito fundamental à privacidade deveria atualizar-se, assegurando proteções jurídico-sociais aos dados pessoais através de novas acepções e garantias.

Daniela Machado e Laura Azevedo (2020) defendem que as mudanças proporcionadas pelo novo modelo de negócio adotado no século XXI influenciam a tal ponto que exigem uma definição do conceito de privacidade que ultrapasse a conceituação tradicional. A justificativa utilizada pelas autoras reside no fato de que a proteção aos dados das pessoas físicas ultrapassa as limitações de cada indivíduo e adentra as da esfera pública.

Bruno Bioni (2021) explica que para o surgimento de uma nova definição de privacidade, dever-se-ia conjugar o direito à privacidade em sua acepção tradicional, que exprime uma liberdade negativa e o direito à proteção de dados, que exprime uma liberdade positiva. Assevera-se ainda que a esfera privada do indivíduo fosse construída, não podendo ser estabelecida de modo fixo e *a priori*, constituindo assim um novo direito que possui o dinamismo como uma de suas características, já que seria construído conforme as necessidades de proteção às informações das pessoas naturais.

Em torno desta conjuntura, surge o direito à autodeterminação informativa. Laura Schertel Mendes (2020, p. 12) explica que, através de decisão do Tribunal Constitucional Alemão, surge sua conceituação. Em resumo, a autora o elucida em três aspectos: primeiro, pelo poder decisório da pessoa física sobre as operações envolvendo seus dados pessoais; segundo, a proteção albergada por esse direito não é fixa, sendo moldada conforme as necessidades e a definição da esfera pessoal-privada de cada um; terceiro, “a referência

pessoal do dado atua decisivamente sobre o teor da proteção na medida em que cada registro que se revela como pessoal é merecedor de proteção".

Fabrizio Lima Silva (2021) elucida que o direito à autodeterminação informativa foi elevado à categoria de fundamental pela primeira vez em uma Constituição no ano de 1976, em Portugal. O autor elenca essa inserção como uma nova roupagem para o direito à privacidade, na qual há o direito de determinação da esfera pessoal, particular, pela própria pessoa física, assim como também o seu direito em vistoriar como suas informações pessoais estão sendo utilizadas.

Assim, o direito à autodeterminação informativa expressa uma evolução, uma atualização, um *upgrade* do conceito fundamental de privacidade, garantindo o poder do indivíduo sobre aquilo que está inserido em sua esfera de intimidade. Contudo, algumas considerações devem ser traçadas.

Embora a autodeterminação informativa represente uma evolução da privacidade, não poderá ser confundida com esta, uma vez que carrega em si, garantias e características que a distancia do direito à privacidade. Também traz consigo elementos que a assimilam e a aproximam de outros direitos tradicionais, como os direitos à personalidade, de maneira que também pode ser considerada uma evolução deste último.

Importantes considerações no que se refere à diferenciação entre a privacidade e a autodeterminação informativa são feitas por Bruno Bioni (2021, p. 95):

Há, portanto, uma série de liberdades individuais, atreladas ao direito à proteção dos dados pessoais, que não são abraçadas pelo direito à privacidade. Além disso, o centro gravitacional da proteção dos dados pessoais é diferente do direito à privacidade – i.e., a percepção de que a sua tutela jurídica opera fora da dicotomia do público e do privado. O direito à proteção dos dados pessoais deve ser alocado como uma nova espécie do rol aberto dos direitos da personalidade, dando elasticidade à cláusula geral da tutela da pessoa humana. Caso contrário, corre-se o risco de ele não se desprender das amarras conceituais e da dinâmica do direito à privacidade e, em última análise, inviabilizar uma normatização própria para regular o fluxo informacional como fator promocional da pessoa humana.

Seguindo posicionamento semelhante, Maria Cachapuz (2014) aduz que a autodeterminação informativa e a esfera pública das informações pessoais garantem também o livre desenvolvimento da personalidade na sociedade contemporânea. Laura Mendes (2020) assevera que o direito à autodeterminação informativa é uma forma de garantia da proteção da personalidade, através da preservação do poder de decisão e de seus instrumentos de procedimento para a pessoa natural.

Joana Machado (2014) identifica o direito à privacidade como parte tanto do rol dos direitos fundamentais como também da personalidade. A autora ainda esclarece que o direito à autodeterminação informativa é explicitado como pré-requisito para o exercício da cidadania na era eletrônica. Também defende que o direito à autodeterminação informativa representa apenas parte do direito à privacidade atual, sendo fruto de uma interpretação mais ampla tanto deste último direito como o da personalidade. Por fim, Machado (2014, p. 361) indica que os avanços tecnológicos forçaram um novo enfoque à privacidade, que a autora denomina de “privacidade informacional”.

Interessa salientar que as leis protecionistas de dados carregam em si tanto a privacidade e intimidade em suas acepções tradicionais, bem como também nos direitos relacionados ao desenvolvimento da personalidade e do *upgrade*: direito à autodeterminação informativa. O caso brasileiro é um exemplo desse aspecto, já que a Lei Geral de Proteção de Dados os elenca em seus fundamentos.

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

I - o respeito à privacidade;

II - a autodeterminação informativa;

[...]

IV - a inviolabilidade da intimidade, da honra e da imagem;

[...]

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (BRASIL, 2018a)

Mediante o exposto, pode-se inferir que o direito à privacidade em sua acepção clássica sofreu determinadas alterações para adequar-se às mudanças ocasionadas na sociedade, com destaque para os avanços tecnológicos. Nesse contexto, a economia passa a ter os dados relativos a pessoas naturais como elementos centrais de seu desenvolvimento. Ocorre que esses dados, por conterem informações relativas aos indivíduos, também fazem parte de sua esfera privada, de sua intimidade, de modo a merecer proteção amparada pelo direito à privacidade.

Aliado a isso, surge o direito à autodeterminação informativa. Este assegura que a pessoa física tenha poder e controle sobre seus dados pessoais e operações envolvendo-os, de maneira a ter proteção jurídica conforme a necessidade de cada sujeito, incluindo até mesmo àquela que inclui as referências a essas informações pessoais. Pode ainda ser entendido como uma evolução do direito à privacidade, não podendo, porém, ser confundido ou resumido pelo mesmo, haja vista que possui características peculiares. Em síntese, a autodeterminação

informativa possui aspectos que o classificam como uma espécie de atualização, de *upgrade* tanto do direito à privacidade, como também do direito à personalidade.

4.3 Antecedentes à proteção brasileira de dados

Verifica-se que o Direito, como ciência social aplicada que é, busca regular as relações inseridas na sociedade, de modo a garantir o equilíbrio, a harmonia, a justiça social e a segurança jurídica aos indivíduos à sociedade como um todo. Como os dados passaram a representar um poder, um valor, uma mercadoria para as empresas, então coube ao direito a tarefa de instituir mecanismos a fim de protegê-lo.

Patrícia Peck Pinheiro (2016) classifica a proteção às propriedades do indivíduo, bem como de sua privacidade como indiscutível e ainda acrescenta que a liberdade de informação encontra alguns de seus limites pelo direito fundamental à privacidade. Por fim, a autora também classifica as informações (dados) pessoais como uma espécie de propriedade, haja vista que o modelo de negócios do século XXI adota os dados não apenas como um produto, uma riqueza, mas também como uma moeda de troca, de pagamento.

Todavia, deve-se fazer uma consideração: os dados pessoais possuem seu valor econômico, apesar de não poderem resumir-se à esfera patrimonial. Danilo Doneda (2020b) afirma que alguns consideram as informações de cunho pessoal como um bem que pode ser regulado pelo direito privado de modo análogo à propriedade. Contudo, adverte-se que tal designação é incompleta, embora solucione problemáticas envolvendo os dados pessoais, haja vista que eles são permeados por diversos interesses que não podem resumir-se aos aspectos monetários.

Ana Sanden (2014) rememora que surgiram, na década de 1960, alguns projetos envolvendo operacionalização de dados pessoais que despertaram a atenção dos juristas das mais influentes democracias mundiais, com destaque para os Estados Unidos e os países europeus. Neste momento, surgiram as primeiras preocupações envolvendo a destinação das informações pessoais coletadas pelo governo ou por instituições privadas, de maneira que a discussão ganha maior amplitude na década seguinte, no Conselho da Europa.

Segundo a Agência dos Direitos Fundamentais da União Europeia e o Conselho da Europa (2018), este último foi criado após a Segunda Guerra Mundial e reúne países europeus de modo a promover, dentre outros objetivos, os direitos humanos e o desenvolvimento social. Para isso, foi criada a Convenção Europeia dos Direitos do Homem (CEDH), cuja vigência iniciou-se em 1953. Neste documento, através de seu artigo 8º, é encontrado e

garantido o direito à proteção de dados pessoais, através da proteção e respeito à vida privada. Além disso, a partir de década de 1970, o Conselho da Europa passou a emitir diversas resoluções sobre a proteção de dados (com fulcro no artigo 8º da CEDH), destacando-se a Convenção 108, cuja assinatura fora aberta em 1981, sendo o primeiro instrumento internacional juridicamente vinculativo sobre a temática.

Paralelamente ao ambiente europeu, os Estados Unidos também vivia seus primeiros desafios e experiências envolvendo a utilização de dados pessoais. Neste cenário, surge a discussão, inclusive através de audiências no congresso norte-americano, a respeito do projeto de uma central de banco de dados nacional, segundo assevera Danilo Doneda (2020a). O autor relembra que, após intenso debate a respeito do projeto, surgiram as primeiras leis sobre a temática: em 1970, o *Fair Credit Reporting Act* (FCRA), lei que relacionava os dados pessoais e o crédito; em 1974, o *Privacy Act*, que regulava o tratamento de dados pessoais por entidades governamentais. Todavia, o escritor alerta que a lei proposta naquela década que possui maior importância para a contemporaneidade foi: *Records, Computers and the Rights of Citizens*, já que estipulou alguns princípios que são utilizados pelas legislações protetivas de dados atuais: transparência, finalidade, livre acesso, entre outros.

Outras legislações ao redor do mundo também marcaram a conjuntura da proteção de dados na década de 1970, conforme indica Ricardo Villas Bôas Cuêva (2016, p. 10):

Na década de 1970, surgem as normas de proteção de dados pessoais de primeira geração, como a lei do Land alemão de Hessen (1970), a lei de dados da Suécia (1973), o estatuto de proteção de dados do Land alemão de Rheinland-Pfalz (1974) e lei federal de proteção de dados da Alemanha (1977). Nos EUA, foi editado, em 1970, o Fair Credit Reporting Act e, em 1974, o Privacy Act. Em 1976, Portugal foi o primeiro país a estabelecer em sua constituição o direito fundamental à autodeterminação informativa (art. 35).

Nathalie Marthial-Braz (2018) destaca também um julgado europeu. A autora faz referência à decisão do Tribunal Constitucional Alemão que, em 1983, através de interpretação constitucional no caso do recenseamento populacional feito pelo poder público, assegurou o direito da pessoa natural em ter ciência a respeito do uso de seus dados, bem como o poder de decidir sobre como e se poderá ser feito, estabelecendo a gênese do direito à autodeterminação informativa. Érica Soares D'Almeida (2020) salientou que a referida decisão utilizou como parâmetro o princípio da dignidade humana.

Enfim, surgiram inúmeras legislações, decisões, precedentes no que se refere à temática deste capítulo. Contudo, o cenário mundial da proteção de dados pessoais atingiu um

nível de extensão maior com o surgimento do GDPR (*General Data Protection Regulation*), também conhecido como RGPD (Regulamento Geral sobre a Proteção de Dados). A mencionada lei salvaguardou os direitos relacionados à defesa da proteção dos dados pessoais de forma ampla, sendo aplicável em todo o continente europeu.

Dentre os precedentes do GDPR, Danilo Doneda (2020a) destaca a adoção da Diretiva 95/46/CE, que fora aprovada pelo parlamento europeu e era válida para todo o velho continente. O escritor ainda pontua que sua validade permaneceu até a aprovação do GDPR, que a substituiu.

Com fulcro em seu artigo 1, itens 1 e 2, os objetos da Diretiva 95/46/CE (UNIÃO EUROPEIA, 1995) eram:

- 1 . Os Estados-membros assegurarão, em conformidade com a presente directiva, a protecção das liberdades e dos direitos, fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais.
- 2 . Os Estados-membros não podem restringir ou proibir a livre circulação de dados pessoais entre Estados--membros por razões relativas à protecção assegurada por força do n° 1.

Patrícia Peck Pinheiro (2021) assegura que o início de debate que culminou no GDPR foi feito pelo partido *The Greens*. A escritora também explica que, embora o GDPR tenha sido promulgado em 27 de abril de 2016, houve previsão de dois anos para que os países se adequassem, de modo que a aplicação de penalidades previstas na lei só seria feita a partir de 25 de maio de 2018.

Por fim, Peck Pinheiro (2021) sustenta que o início da vigência provocou o início de um “efeito dominó” a nível internacional, haja vista que fora estabelecido um nível de proteção de dados pessoais que deveria ser acatado pelos países que desejassem realizar relações comerciais com os europeus. Ou seja, a adoção de legislações protetivas de dados, em nível semelhante ou superior ao do GDPR, pode ser entendida como pressuposto necessário para aqueles que desejem manter suas importações e exportações com os países do velho continente.

Assim como no caso da Diretiva 95/46/CE, os itens 1, 2, 3 do artigo 1 do GDPR (UNIÃO EUROPEIA, 2016) também explicita seus objetos:

1. O presente regulamento estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

2. O presente regulamento defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais.
3. A livre circulação de dados pessoais no interior da União não é restringida nem proibida por motivos relacionados com a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais.

Indra Spiecker Gen. Döhmann (2020) elenca alguns princípios básicos do GDPR. Princípios do estabelecimento e do local do mercado, aquele se referindo à aplicabilidade do GDPR para todo e qualquer estabelecimento presente na União Europeia (UE) que trate dados e, este, sendo substituto do tradicional princípio da territorialidade, estabelece que haja aplicação do GDPR quando houver oferecimento de bens ou serviços na UE ou ainda quando envolver pessoas presentes na UE. Já o princípio da proibição estabelece que não possa haver operacionalização de dados quando não houver uma justificativa para isso, incluindo-se operações seguintes a uma feita com determinada justificativa (há necessidade de estabelecimento de nova justificação).

Gen. Döhmann (2020) também elenca o princípio da vinculação à finalidade, que está intrinsecamente ligado ao princípio da proibição, de modo a garantir que as operações envolvendo dados devem ser feitas sob uma finalidade certa e previamente informada. A transparência também detém sua importância para o GDPR, uma vez que a pessoa física tem o direito de livre acesso a todas as informações relacionadas ao tratamento de seus dados, cabendo, àquele que realiza os procedimentos, o dever de prestar informações claras e precisas. Pode-se citar também o princípio da parcimônia ou da minimização de dados, relacionados ao princípio da finalidade, de maneira que esta deverá ser atendida na menor número de operações possíveis, evitando-se futuros tratamentos sem justificativa.

Ressalta-se, por fim, que os princípios do GDPR estão explicitados no capítulo II do regulamento, de modo a ser abarcado entre os artigos 5 e 11.

Por fim, ressalta-se que os princípios contidos no GDPR, como também toda sua estruturação, institutos e ainda o “efeito dominó” por ele provocado, possuem claros reflexos na Lei Geral de Proteção de Dados. Esta última caracteriza-se como a principal lei que garante e regula a proteção de dados pessoais no Brasil atualmente.

4.4 A proteção dos dados no Brasil

Na verdade, o Brasil careceu de leis específicas de proteção de dados por muitos anos. Para sanar tal omissão, intentava-se proteger as informações pessoais das pessoas físicas através de institutos esparsos contidos no ordenamento jurídico.

Danilo Doneda (2020b, p. 266) entende que o desenvolvimento histórico da proteção de dados brasileira anterior à Lei Geral de Proteção de Dados (LGPD), deu-se através do que ele denomina de “cláusula geral da personalidade”. O autor também explica que a Constituição, pelos incisos de seu artigo 5º, instituiu algumas garantias ligadas à privacidade, ainda que não relacionadas – expressamente – aos dados pessoais: inviolabilidade da vida privada e intimidade (X), inviolabilidade de comunicações telefônicas, telegráficas ou de dados (XII), *habeas data* (LXXII), entre outros. Por fim, o também se afirma que existiam algumas disposições no ordenamento jurídico relativas, indiretamente, aos dados pessoais através de leis de outras naturezas, como no âmbito do direito civil, penal, comercial e processual.

No que tange à legislação dispersa, Ana Sanden (2014) destaca os artigos 43 e 44 do atual Código de Defesa do Consumidor. A autora assegura que o rol presente nesses artigos prevê direitos, ligados à proteção de dados, mais abrangentes que os garantidos pela Constituição Federal através do *habeas data*, e ainda apresenta alguns deveres àquele responsável pelo banco de dados ou cadastro. A escritora também identifica alguns institutos presentes no artigo 43, que segue abaixo, que são muito semelhantes aos mecanismos protetivos de dados contemporâneos: *caput* apresenta o livre acesso à informação; parágrafo 3º apresenta o direito à retificação da informação; parágrafos 1º e 5º garantem o direito ao esquecimento; parágrafo 1º assimila ainda os princípios da exatidão, transparência e também uma espécie de temporalidade do uso.

Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

§ 1º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.

[...]

§ 3º O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.

[...]

§ 5º Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores. (BRASIL, 1990a)

Danilo Doneda (2020b) explica que os supracitados artigos do Código de Defesa do Consumidor foram precursores e previam princípios implícitos previstos na legislação europeia de proteção de dados (GDPR), introduzidas em uma sistemática singular: a da proteção consumerista. O autor também salienta a intenção do legislador em instituir um equilíbrio na relação de consumo através da imposição de balizas ao uso de dados a respeito do consumidor, guardando por isso também, outra semelhança com leis protecionistas de dados pessoais.

Laura Schertel Mendes (2019) relembra diversas outras legislações que construíram, ainda que com enfoque em outros ramos do direito, a proteção de dados no Brasil: Lei de Acesso à Informação, Lei do Cadastro Positivo, Código de Defesa do Consumidor, Marco Civil da Internet.

Guimarães Filho, Ferneda e Ferraz (2018) enfatizam e defendem que a lei nº 2.965/14, mais conhecida como Marco Civil da Internet (MCI), demonstrou a oposição existente entre a privacidade e as práticas de tratamento de dados desreguladas. Pontua-se ainda que a proteção de dados criada pelo MCI fora sistemática, especialmente no que se refere a seu artigo 7º e toda sua seção II, esta sendo direcionada especificamente sobre o tema. Sobre o citado artigo, destaca-se seu inciso VII e suas alíneas:

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

[...]

VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

- a) justifiquem sua coleta;
- b) não sejam vedadas pela legislação; e
- c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; (BRASIL, 2014)

Alexandre Libório Pereira (2016, p. 54) recorda que o MCI foi considerado como a “Constituição da Internet”. Além disso, também destacou aqueles que são considerados como os pilares do MCI, com destaque para o segundo, que está relacionado à “proteção da privacidade e dos dados pessoais”.

Ademais, outro importante instituto teve vital importância para a defesa da proteção de dados desde a promulgação da Constituição Federal de 1988 (CF): trata-se do *habeas data*, cuja previsão é explicitada no inciso LXXII do artigo 5º da CF:

[...]

LXXII - conceder-se-á "habeas-data":

- a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
- b) para a retificação de dados, quando não se prefera fazê-lo por processo sigiloso, judicial ou administrativo; [...]. (BRASIL, 1988).

Manoel Gonçalves Ferreira Filho (2020) explica que o *habeas data*, resumidamente, possui dois escopos: retificação de dados e conhecimento de informações. Assevera que deve ser utilizado de modo a manter compatibilização com os incisos do art. 5º: XII (inviolabilidade do sigilo de dados), XXXIII (direito de petição), XXXIV, alínea b (direito à obtenção de certidões).

José Carlos Barbosa Moreira (1998) salienta a notoriedade do conhecimento e da retificação de dados proporcionada pelo *habeas data*. O autor defende que sua dimensão protetiva é fundamental para os direitos à intimidade e privacidade, classificando como invasiva a coleta e armazenamento de informações pessoais sem qualquer controle pela pessoa a quem os dados se referem.

Alexandre de Moraes (2021) aponta que o surgimento do *habeas data* deu-se através do *Freedom of Information Act* de 1974, lei oriunda dos Estados Unidos e que garantia o acesso da pessoa física a dados contidos em registros públicos. O autor ainda aduz que, embora seja uma ação constitucional, possui caracterização civil. Também se explicita que seus procedimentos estão previstos na Lei nº 9.507/97 e que o processo de *habeas data* terá prioridade sobre os demais, exceto *habeas corpus* e mandado de segurança.

Barbosa Moreira (1998, p. 3) ainda advoga que o rol protetivo do *habeas data* fora fundamental para uma mudança de panorama relativa ao retorno do Estado de Direito, em oposição às décadas anteriores. Estas foram marcadas por “regimes políticos de exceção” e “governos discricionários” que inseriram informações duvidosas e muito discutíveis, impossibilitando ainda o acesso aos dados inseridos, tornando igualmente impossível a prova da falsidade dos mesmos, provocando um cenário kafkiano de desrespeito a direitos.

Laura Schertel Mendes (2019) defende que, conquanto o *habeas data* proteja as informações pessoais, seu principal papel jurídico é a defesa contra desvios na

operacionalização de dados. Assim, garante à pessoa natural que as informações coletadas sejam fidedignas e utilizadas apenas para fins lícitos, legítimos e não discriminatórios. Por isso, a autora explica que o *habeas data* coaduna totalmente com o direito à autodeterminação informativa, de maneira que aquele é a garantia processual de proteção à privacidade e personalidade do indivíduo através de seus dados, e este seria o próprio direito que protege a pessoa natural de procedimentos ilegítimos em seus dados.

O entendimento da importância da dimensão protetiva do *habeas data*, em relação à proteção de dados pessoais, privacidade e personalidade, não era defendido apenas pela doutrina. Marco Aurélio Bellizze Oliveira e Isabela M. Pereira Lopes (2020) explicam que esse ponto de vista era também explicitado pelos tribunais superiores desde a década de 1990. Para isso, os autores destacam os julgamentos do: Recurso Ordinário em Habeas Data (RHD) 22/DF, no qual os ministros Sepúlveda Pertence e Celso de Mello defenderam o uso do *habeas data* como fulcral para a proteção de dados; e do Recurso Especial 11.337-9/RS, cuja relatoria fora incumbida ao Ministro Ruy Rosado de Aguiar Júnior.

Em torno do apresentado, é interessante avaliar que o ordenamento jurídico, ao longo do tempo, proporcionou a proteção de dados, ainda que restrita e incompleta, através de alguns dispositivos normativos esparsos. Encontraram-se princípios implícitos, como os previstos no Código de Defesa do Consumidor; explícitos, como os previstos no Marco Civil da Internet e ainda ações materiais para proporcionar a efetivação da proteção de dados como a do *habeas data*.

Para complementar esse cenário, em que a proteção de dados pessoais caminhou a passos curtos, surge a Lei Geral de Proteção de Dados (LGPD). Fora a primeira legislação específica sobre a operacionalização de informações de pessoas físicas no Brasil, de maneira a proporcionar mecanismos, institutos, princípios semelhantes ao padrão adotado pela legislação europeia.

Após o início da vigência da LGPD, também emergiram algumas iniciativas para tornar a proteção de dados ainda mais relevante para o direito nacional. Dentre elas, destaca-se a Proposta de Emenda à Constituição (PEC) n°17/2019 que, segundo Pedro Pincer (2021), fora aprovada e aguarda sua promulgação em sessão do Congresso Nacional.

5 LEI GERAL DE PROTEÇÃO DE DADOS

O avanço da globalização e das tecnologias proporcionou uma conectividade jamais encontrada pela sociedade. Neste contexto, os dados pessoais ganham elevada notoriedade, caracterizando-se tanto como uma mercadoria com valor econômico, como também parte integrante da personalidade e privacidade das pessoas a quem eles se referem.

Como podem ser tratados como uma mercancia e ainda carregarem características inerentes à pessoa natural, os dados pessoais também merecem sua proteção no ordenamento jurídico. Por isso, surgiram inúmeras leis ao redor do mundo que almejam protegê-los. Dentre elas, destaca-se o GDPR, regulamento europeu que regula e determina a proteção de dados de pessoas físicas no velho continente.

Ocorre que esse dispositivo normativo criou um efeito dominó em outros países que desejassem manter relações comerciais com os integrantes da União Europeia. Ambiente no qual o Brasil também integra, de maneira que buscou criar legislação específica para a proteção de dados pessoais, de modo semelhante ao GDPR. Com isso, em 2018, a Lei Geral de Proteção de Dados (LGPD) é sancionada.

Para compreender melhor a LGPD, pretende-se analisar a sua tramitação legislativa, de forma a elucidar alguns pontos históricos que culminaram em seus dispositivos. Para integralizar as explicações, também serão elucidados os princípios e bases legais que o empregador deverá atender integralmente quando realizar operações sobre os dados de seus empregados.

5.1 Histórico: tramitação legislativa e o efeito dominó

A Lei Geral de Proteção de Dados, também denominada como LGPD, ou Lei nº. 13.709/2018, foi sancionada em 14 de agosto de 2018 pelo então Presidente da República Michel Temer. A mencionada legislação fora a responsável por salvaguardar os direitos relacionados à proteção de dados de pessoas naturais, tendo alterado disposições da lei nº 12.965, o Marco Civil da Internet, consoante notícia Helton Gomes e Márcio Padrão (2018).

Todavia, sua vigência deu-se somente a partir de 18 de setembro de 2020. Por outro lado, conforme Mirthyani Bezerra (2020) assevera, as sanções impostas pela LGPD, que podem ser determinadas no patamar de 2% do faturamento até o limite de 50 milhões de reais, só puderam ser cobradas e executadas a partir de primeiro de agosto de 2021.

Consoante seu caráter protecionista em relação aos dados de pessoas naturais, a Lei Geral de Proteção de Dados também surgiu por outras motivações. Neste sentido, destaca-se o anseio mercadológico e a inserção do país na era da mercantilização digital, em que os dados são os elementos centrais da economia. Essas preocupações são elencadas no próprio texto da LGPD (BRASIL, 2018a): “Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: [...] V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; [...]”.

Milton Monti foi o deputado responsável pela elaboração do Projeto de Lei (PL) nº4060 de 2012, que futuramente seria a LGPD. Em vista da época em que fora proposto, e do modo com que o PL fora estruturado, é possível afirmar-se que houve uma grande influência da Diretiva 95/46/CE, já mencionada em capítulo anterior.

Na justificativa do projeto inicial, Milton Monti (2012, p. 7) explica que o desenvolvimento tecnológico fez urgir a necessidade de uma regulamentação que proporcionasse a garantia da privacidade das pessoas físicas e também da livre iniciativa de mercado e de comunicações. Ainda afirma que a ideia do projeto surgiu através do V Congresso Brasileiro da Indústria da Comunicação em que o deputado era presidente da seção responsável pela discussão da privacidade e personalização. Por fim, cita-se ainda que a organização do congresso foi feita pela “ABAP – Associação Brasileira das Agências de Publicidade e pelo FORCOM – Fórum Permanente de Comunicação” e que a discussão em sua comissão contou com a presença de algumas personagens ilustres: “blogueiro Marcelo Tás, do ator Odilon Wagner, do Presidente da ABEMD Efraim Kapulski, do Advogado Vitor Morais de Andrade, do Diretor da Editora Abril Fernando Costa”, entre outros.

Conforme análise da tramitação feita na Câmara dos Deputados (BRASIL, 2012), pode-se observar que houve muitos percalços para que a aprovação do PL fosse feita. A título de exemplo, pode-se evidenciar que não houve qualquer tramitação entre 21 de agosto de 2013 e 31 de janeiro de 2015, sendo que nesta última ocasião o PL fora arquivado. Vários também foram os deputados relatores do projeto: em 22 de agosto de 2013, fora designado Nelson Marchezan Junior (PSDB-RS); a partir de 11 de março de 2015, Sergio Zveiter (PSD-RJ); já em 12 de novembro de 2015, Sóstenes Cavalcante (PSD-RJ); e por fim, a partir de 26 de outubro de 2016, Orlando Silva (PCdoB-SP).

Interessa também examinar os pareceres emitidos ao longo de toda a tramitação. Em 04 de maio de 2016, fora apresentado parecer do Deputado Sóstenes Cavalcante a respeito da análise e trabalhos realizados pela Comissão de Ciência e Tecnologia, Comunicação e Informática (CCTCI). Pode-se observar que Cavalcante (2016, p. 3-4) enfatizou o caráter

protetivo da lei, mas também a sua importância para a regulação das atividades comerciais envolvendo dados pessoais, de modo que considerou a possível aprovação do PL como um “marco legal contemporâneo” que equipararia a proteção de dados brasileira a de outros países, com realce para a Diretiva 95/46/CE, aplicável no continente europeu.

No parecer de Cavalcante (2016), defende-se a aprovação do PL, e também se sugerem propostas de quatro emendas: aos artigos 6º, 13, 14, 16 e 19. Salienta-se a proposição feita na emenda nº 3, que garantiria o direito à pessoa a quem os dados se referem de solicitar a retirada de seus dados pessoais dos bancos de dados, e a consequente interrupção das operações que os envolvem. A ênfase dada nessa mudança justifica-se pela garantia do direito à privacidade e da autodeterminação informativa, já que salvaguarda o direito da pessoa em controlar e acompanhar o uso de suas informações pessoais.

Em 24 de maio de 2018, fora apresentado novo parecer, perante comissão composta para esse feito e posteriormente, também a todo o plenário. A sua análise fora mais detalhada, sendo feita sobre cada artigo do PL, mas também das onze emendas propostas pelos parlamentares e ainda houve menção às vinte contribuições recebidas de diversos setores e, por fim, houve apresentação de um texto legal substitutivo ao PL inicial.

Em uma contextualização internacional, o novo relator, Deputado Orlando Silva (2018), realçou a legislação europeia sobre proteção de dados e a mudança ocorrida com o surgimento do *General Data Protection Regulation* (GDPR), substituindo a antiga Diretiva 95/46/CE, mas também sobre leis e tratados firmados pelos Estados Unidos e, por fim, mencionou-se o controle feito pela China.

Em relação aos países geograficamente mais próximos, destacou-se a Argentina, que já possui regulamentação sobre o tema e uma autoridade nacional específica para fiscalizar e sancionar as atividades envolvendo proteção de dados, motivo pelo qual o país fora o primeiro latino-americano a receber “[...] a certificação da União Europeia como ‘país adequado’” (SILVA, 2018, p. 11). Neste último ponto, vê-se claramente a força da criação do GDPR e um efeito dominó provocado pelo seu surgimento, no cenário comercial mundial comentado no capítulo anterior.

Em 14 de agosto de 2018, o PL foi transformado em lei: a LGPD. Entretanto, a sanção presidencial (BRASIL, 2018b) também exarou veto a determinados dispositivos da proposta da Câmara dos Deputados, dos quais se destacam dois. O primeiro refere-se ao inciso II do artigo 23, que previa a proteção dos dados dos requerentes da Lei de Acesso à Informação, e que fora vetado pela justificativa de serem dados necessários à execução de políticas públicas (como no caso da Previdência Social), e também às investigações ligadas ao Sistema

Financeiro Nacional. O segundo diz respeito aos artigos 55 a 59 que criavam a autoridade fiscalizadora da proteção de dados (Agência Nacional de Proteção de Dados – ANPD), por motivos de inconstitucionalidade no rito legislativo atinente à matéria.

Consoante o veto realizado pelo presidente, em 2019 o mesmo fora relativizado, em partes, pelo legislativo. Isso ocorre pelo fato de a Lei n° 13.853/2019 ter alterado a LGPD para incluir a ANPD, que restou caracterizada como órgão com autonomia técnica e decisória. Importante ressaltar que houve preocupação da lei quanto às questões orçamentárias da criação da ANPD:

Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República.
 § 1º A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República. (BRASIL, 2019a)

Pelo que fora analisado neste capítulo, algumas considerações interessantes podem ser salientadas em torno de toda a tramitação do PL n°4060/2012, que viria a tornar-se a Lei Geral de Proteção de Dados. Embora a preocupação com a proteção de dados em sua acepção garantidora de direitos fundamentais (privacidade e autodeterminação informativa) fosse presente desde a gênese do PL em 2012, as atenções eram divididas também com relação ao apelo mercadológico da lei.

Como relatado em capítulos anteriores, a criação do GDPR surtiu um efeito dominó no comércio internacional, impondo - indiretamente - a adoção de leis protetivas de dados pessoais em todo planeta e, principalmente, aos países que desejassem realizar comércio com o continente europeu. A LGPD também está inserida neste contexto. Tal fato pode ser verificado pela própria tramitação do PL n°4060/2012: até o ano de 2016 (ano em que a GDPR fora aprovada), três relatores já haviam sido designados, poucas tramitações efetivas foram realizadas e ainda houve arquivamento do PL.

Todavia, a aprovação do GDPR em 2016 deu vida ao efeito dominó, de modo que as tramitações legislativas intensificaram-se. Outra consequência do mencionado efeito é o ano de aprovação da LGPD: 2018, mesmo ano do início da vigência do GDPR. Conforme supramencionado, tanto na justificativa do PL, quanto nos dois relatórios apresentados pelos Deputados relatores Sóstenes Cavalcante e Orlando Silva, havia menção às necessidades de adequação ao mercado internacional. Assim, resta cristalino que, embora tenha cunho

assegurador de direitos fundamentais, a LGPD também possui forte caráter mercadológico, que não pode ser desconsiderado quando analisado o contexto histórico.

5.2 Definições Gerais e Preceitos Essenciais

A Lei Geral de Proteção de Dados (LGPD) inaugurou um novo ramo jurídico no Brasil, haja vista que se trata de uma lei inovadora e geral, não especial. Pelo fato de a seara de proteção de dados ser nova no país, algumas considerações iniciais são essenciais para que haja o entendimento dos preceitos apregoados pela lei. Assim, o presente trabalho pretende esmiuçar alguns conceitos trazidos pela própria LGPD que são cotidianos e fundamentais para o assunto.

Além disso, pretende-se apresentar os pilares sobre os quais a LGPD foi construída. Logo, serão demonstrados os princípios que devem ser atendidos por todo e qualquer empregador quando do tratamento de dados de seus empregados. Ademais, para que as operações envolvendo os dados pessoais do empregado sejam legítimas, devem-se escolher as corretas hipóteses autorizativas elencadas pela lei.

5.2.1 Conceitos

A Lei Geral de Proteção de Dados (LGPD) foi um marco legal na história legislativa brasileira, de modo a ser caracterizada como a primeira lei a tratar, expressa e especificamente, sobre a proteção de dados pessoais. Em vista disso, como toda novidade teórica legislativa, é de suma importância que o embasamento e o texto legal sejam os mais cristalinos possíveis, de modo a garantir uma interpretação e aplicação da lei mais confiável e fiel às intenções inicialmente propostas pelo poder legislativo.

Com isso, evita-se o surgimento de ambiguidades e dúvidas, de maneira a garantir maior segurança jurídica para a própria lei e seu âmbito de funcionamento. Patrícia Peck Pinheiro (2021, p. 16) aduz que o esclarecimento de conceitos feito pela lei é essencial para haver “harmonização em documentos, com especial atenção às políticas, às normas, aos procedimentos e aos contratos”.

Tendo em vista estas considerações, a própria LGPD buscou agir doutrinariamente através dos próprios dispositivos legais, contendo assim explicações de termos utilizados. Em relação aos conceitos trazidos pela lei, o artigo 5º da LGPD (BRASIL, 2018a) buscou defini-los através de seus incisos. Importa analisar alguns deles, pois passarão a ser utilizados

também nesse trabalho após as suas devidas apresentações. Outros termos serão explicados ao longo do trabalho, em oportunidades específicas, demonstrando suas aplicabilidades em casos cotidianos.

O primeiro inciso (BRASIL, 2018a) busca caracterizar o termo “dado pessoal” como sendo aquelas informações relativas às pessoas naturais já individualizadas ou passíveis de serem identificadas. Patrícia Peck Pinheiro (2021, p. 16) explica que os dados farão alusão a pessoas naturais vivas, citando ainda alguns exemplos: “nome, sobrenome, apelido, idade, endereço residencial ou eletrônico, podendo incluir dados de localização, placas de automóvel, perfis de compras, número do *Internet Protocol* (IP), dados acadêmicos, histórico de compras, entre outros”.

Rony Vainzof (2020, p. 82) caracteriza o conceito de dado pessoal da LGPD como “expansionista”, assim como é o do GDPR, uma vez que ambas as leis consideram como dado pessoal aquele em que o indivíduo é expressamente identificado (indivíduo determinado), e também aquele em que seria possível a identificação após certa pesquisa (indivíduo determinável). Por isso, o autor divide os dados pessoais – em sentido estrito – como sendo diretos (pessoas já identificadas neles) e indiretos (pessoas suscetíveis de identificação).

Como exemplo, no caso do dado pessoal direto, podem-se citar digitalizações da Carteira de Trabalho e Previdência Social (CTPS) do trabalhador, já que este é identificado pelo nome e foto 3x4 constantes no documento. Por outro lado, se repassado apenas o número da CTPS, será evidenciado um dado pessoal indireto, já que, embora não seja possível a identificação direta da pessoa natural através do número, após breve análise, seria possível sua identificação, como no caso de busca em um banco de dados.

O inciso segundo, buscar criar um conceito através de exemplos:

[...]

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; [...]. (BRASIL, 2018a)

Patrícia Peck Pinheiro (2021) associa os dados pessoais sensíveis a aspectos de personalidade da pessoa natural, bem como suas próprias escolhas. Regina Ruaro e Gabrielle Sarlet (2021, p. 194) admitem que os dados pessoais sensíveis possam ser considerados como “nucleares para a prefiguração e para a personificação do sujeito de direito no contexto atual”.

Por outro lado, Bruno Ricardo Bioni (2021) entende que a terminologia diferenciada (sensíveis) é justificada por um atributo inerente a esses dados: a vulnerabilidade em seu conteúdo. O autor explica que informações como raça, orientação sexual ou religiosa, partes integrantes da personalidade do indivíduo, quando analisadas por determinadas pessoas, poderão ocasionar situações discriminatórias para os indivíduos a quem os dados sensíveis se referem.

Em outro entendimento, Danilo Doneda (2020b) interliga a denominação diferenciada pelos diferentes efeitos provocados por esta classe de dados. Assegura que seu surgimento advém da percepção de que a proteção da privacidade tradicional não seria o suficiente, já que se destaca outro preceito fundamental que merece atenção: igualdade material. A constatação de dados como sendo sensíveis é fruto do potencial lesivo das informações que os diferenciam quando analisadas sob a configuração social em que estão inseridos.

No que concerne ao inciso V, conceitua-se o termo “titular” (BRASIL, 2018a) como sendo aquele que designa a pessoa natural, cujos dados pessoais estão sendo processados. Ou seja, são as pessoas físicas às quais os dados pessoais caracterizam e fazem referência. Rony Vainzof (2020, p. 95) identifica o titular como “[...] núcleo de existência de uma Lei Geral de Proteção de Dados”, haja vista que os cuidados impostos por esse espécime legislativo têm como finalidade a garantia dos direitos fundamentais da pessoa natural, do titular dos dados.

Patrícia Peck Pinheiro (2021) explica que, conquanto as pessoas jurídicas não estejam albergadas pela terminologia explicada no inciso V, o cadastro das mesmas pode conter informações relativas a pessoas naturais. Logo, as operações que as envolvem são dignas de rigorosa atenção no que tange à proteção de dados, como no caso dos Microempreendedores Individuais (MEIs).

No que diz respeito ao inciso X, encontra-se presente a definição do termo “tratamento” que denota e resume toda e qualquer operacionalização envolvendo os dados. Em outras palavras, qualquer atividade realizada com os dados pode ser referida como uma espécie de tratamento. O inciso X cita alguns exemplos de tratamento de dados:

[...] coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. (BRASIL, 2018a).

Ainda cabe destacar a caracterização elencada no inciso XII, que traz explicações a respeito do consentimento: “manifestação livre, informada e inequívoca pela qual o titular

concorda com o tratamento de seus dados pessoais para uma finalidade determinada;” (BRASIL, 2018a). Em outros dizeres, consentimento pode ser entendido como o aceite da pessoa a quem os dados se referem sobre as operações envolvendo seus dados pessoais.

Importante aqui destacar que o consentimento exige alguns requisitos no modo em que deverá ser feito, para que seja considerado válido. São eles: livre, informado e inequívoco. Ressalta-se desde já que essas terminologias serão analisadas com maior atenção nos capítulos seguintes.

Por fim, salienta-se que os incisos XIII e XIV descrevem dois tratamentos específicos envolvendo os dados: bloqueio e eliminação (BRASIL, 2018a). Aquele pode ser sintetizado pela suspensão do uso dos dados pessoais, através da manutenção do dado em si ou do banco de dados, de maneira que poderão ser utilizados futuramente quando permitidos. Por outro lado, a eliminação consiste no apagamento de informações relativas à pessoa natural.

Rony Vainzof (2020) elucida que os procedimentos dos incisos XIII e XIV ocorrerão quando os dados pessoais forem considerados como coletados em excesso (além do mínimo necessário para a finalidade proposta), quando não houver necessidade de sua manutenção, ou ainda quando o tratamento for realizado em desconformidade com a LGPD. O autor ainda evidencia que a suspensão também se enquadra como uma das previsões de sanção da lei, sendo uma opção intermediária em relação às demais e que será aplicada após processo administrativo. No tocante à eliminação, a mesma também é considerada como uma sanção, mas também como um direito do titular dos dados, que poderá solicitar que os dados sejam apagados quando o consentimento for a única base legal de tratamento utilizada, de modo que seu pedido deverá ser acatado.

5.2.2 Princípios

Além da apresentação dos conceitos apontados, a Lei Geral de Proteção de Dados carrega consigo diversos princípios que deverão ser observados quando houver tratamento de dados pessoais. Patrícia Peck Pinheiro (2021, p. 18) elucida que a LGPD, à semelhança do GDPR, pode ser considerada como uma lei "principiológica". Também se explana que os princípios elencados deverão ser atendidos em sua integralidade, já que foram as configurações objetivas criadas para que haja tratamento que respeite, concomitantemente, os direitos fundamentais e ainda os modelos de negócio e suas estruturas.

Patrícia Peck Pinheiro (2021, p. 18) também faz comparações interessantes a respeito da LGPD e GDPR, que possuem grande semelhança principiológica. Em relação ao

regulamento europeu, a autora explica que os princípios encontram-se previstos em seu artigo 5º: “(i) licitude; (ii) lealdade; (iii) transparência; (iv) limitação da finalidade; (v) minimização dos dados; (vi) exatidão; (vii) limitação da conservação; (viii) integridade e confidencialidade (que são os mesmos da segurança da informação); (ix) responsabilidade”.

Contrariamente, a LGPD os prevê em seu artigo 6º. Destarte, os tratamentos deverão ater-se à boa fé, assim como também, à finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas (BRASIL, 2018a). Isto posto, é importante notar que a LGPD não apenas possui princípios semelhantes ao GDPR, como também possui alguns que são idênticos, demonstrando toda a influência do ordenamento jurídico europeu na proteção de dados brasileira.

Bruno Bioni (2021, p. 131) deslinda que os princípios explicitados na LGPD tem seu “centro gravitacional” no titular de dados. Também classifica os princípios em clássicos, como o da transparência e qualidade de dados, e os “modernos” como no caso da adequação e necessidade. Ainda defende que a base de princípios elencada pela LGPD busca conferir maior controle do titular dos dados a respeito de suas informações pessoais, conferir maior autonomia ao mesmo, garantindo a autodeterminação informativa.

Salienta-se que os princípios não são apenas meios dirigentes para o tratamento de dados. Também serão norteadores da interpretação legal, de maneira que a não observância dos mesmos, poderá acarretar em um entendimento que considere o tratamento como ilegítimo ou até mesmo ilegal (por ir contra preceitos contidos na LGPD). Logo, a submissão das operações envolvendo dados pessoais aos princípios contidos na lei é uma condição obrigatória para qualquer tratamento de dados.

5.2.2.1 Boa-fé

O primeiro princípio identificado na LGPD, através do caput do seu artigo 6º (BRASIL, 2018a), é o da boa-fé. Silvano Flumignan e Wévertton Flumignan (2020, p. 125) entendem que a previsão dos demais princípios nos incisos, enquanto o da boa fé está disposto no caput, demonstra que sua importância como “principal princípio norteador da LGPD”. Destacam-se duas vertentes da boa-fé: boa intenção e oposto da má-fé. Este último, no cenário de proteção de dados, pode ser resumido através do não conhecimento a respeito da lesividade do tratamento sobre direitos do titular ou de terceiros, de maneira que qualquer

modo de desrespeito nas operações envolvendo dados pessoais acarretará na deslegitimação ou até ilegalidade do tratamento.

Os autores ainda asseveram que a inserção da boa-fé como princípio norteador da LGPD denota a intenção do legislador em atribuir uma cláusula aberta para a interpretação judiciária, uma vez que entende que a lei não conseguirá regular a integralidade das possibilidades de relações jurídicas e sociais. Nesse ponto, é válido notar que a interpretação baseada na boa-fé também será de suma importância na matéria discutida, já que o tratamento de dados poderá sofrer diversas modificações, tendo em vista que a lei também não conseguirá alinhar-se integralmente ao avanço das tecnologias, que possuem maior velocidade que os avanços do direito.

Diante do exposto, resta o entendimento de que o empregador deverá tratar os dados de seus empregados baseando-se na boa-fé. Supõe-se assim que suas condutas relacionadas às informações pessoais dos trabalhadores deverão, além de estar de acordo com os preceitos legais, demonstrar boas intenções, respeito e prudência.

5.2.2.2 A trindade da finalidade, adequação e necessidade.

Os incisos I, II e III explicitam princípios que estão fortemente interligados: finalidade, adequação e necessidade. O tratamento de dados conforme os dizeres desse “trinômio” pode ser resumido pelos dizeres de Selma Carloto (2021, p. 162):

O tratamento deverá ser realizado com propósitos legítimos, específicos, explícitos e os quais deverão ser informados ao titular, devendo haver a compatibilidade do tratamento com as finalidades informadas ao titular e o tratamento ser limitado ao mínimo necessário, com eliminação de excesso de dados desnecessários para a finalidade específica e informada e de acordo com o contexto do tratamento. Os agentes de tratamento deverão sempre tratar os dados necessários e de acordo com a finalidade. Uma nova finalidade demandará muitas vezes uma nova base legal e todos os tratamentos e finalidades deverão ser informados aos titulares dos dados pessoais ou dados sensíveis.

Rony Vainzof (2020) identifica esses três princípios como integrantes, juntamente com o princípio da transparência, da essência da Lei Geral de Proteção de Dados. Justifica tal posicionamento pelo fato de essa trindade ser a responsável por garantir o atendimento e respeito aos direitos fundamentais do titular.

No tocante ao princípio da finalidade, Danilo Doneda (2011) enfatiza dois aspectos. Primeiro, entende-se que o tratamento de dados deve respeitar, de modo integral e exato, a

finalidade previamente determinada e informada ao titular, para a coleta e as operações envolvendo suas informações pessoais. Segundo, a finalidade deve ser legítima, de maneira a não divergir de outros princípios e determinações da lei, bem como também não ser abusiva.

No que tange à necessidade de dar ciência ao titular dos dados a respeito da finalidade do tratamento, pode-se considerar como uma ampliação de direitos pré-existentes. Marco Aurélio Bellizze Oliveira e Isabela Lopes (2020) afirmam que a obrigatoriedade de prévia notificação sobre o cadastramento já estava previsto no Código de Defesa do Consumidor, tendo sido posteriormente reproduzida pela Lei do Cadastro Positivo e Marco Civil da Internet.

A relação entre o princípio da finalidade, a privacidade e a proteção de dados é necessária, de modo que aquele primeiro garante a menor invasão possível à intimidade do titular dos dados. Esse entendimento já era expresso nos tribunais brasileiros antes mesmo do advento da LGPD. O acórdão do Recurso Especial nº 22.337/RS, de relatoria do Ministro Ruy Rosado de Aguiar, já em 1995, demonstrava que o exercício da proteção ao crédito, através do acesso a informações pessoais deveria ser feito resguardando as limitações impostas pela finalidade determinada, sob pena de ocasionar impacto social negativo maior do que o bem pretendido:

O Serviço de Proteção ao Crédito (SPC), instituído em diversas cidades pelas entidades de classe de comerciantes e lojistas, tem a finalidade de informar seus associados sobre a existência de débitos pendentes por comprador que pretenda obter novo financiamento. É evidente o benefício que dele decorre em favor da agilidade e da segurança das operações comerciais, assim como não se pode negar ao vendedor o direito de informar-se sobre o crédito do seu cliente na praça, e de repartir com os demais os dados que sobre ele dispõe. Essa atividade, porém, em razão da sua própria importância social e dos graves efeitos dela decorrentes – pois até para inscrição em concurso público tem sido exigida certidão negativa no SPC – deve ser exercida dentro dos limites que, permitindo a realização da sua finalidade, não se transforme em causa e ocasião de dano social maior do que bem visado. (BRASIL, 1995).

Ana Sanden (2014) explica que a coleta e demais formas de tratamento de dados deverão ater-se, rigorosamente, aos limites impostos pela finalidade específica que motivou cada uma das operações envolvendo os dados. Para que isso seja alcançado, a descrição da finalidade deve ser objetiva, clara, evitando-se ambiguidades. Por isso, o empregador, ao tratar os dados de seus empregados, deverá atuar de modo atencioso para garantir que a finalidade inicial não seja distorcida, alterada, sob pena de deslegitimar o tratamento feito.

Flumignan e Flumignan (2020), com base no artigo 9º, parágrafo 2º, da LGPD fazem considerações interessantes. Explicam que caso seja requerido o consentimento do titular a respeito da finalidade inicialmente especificada e ela seja alterada, o titular será informado das modificações, tendo ainda o direito de não aceitá-las e revogar seu consentimento, de modo que o empregador deverá cessar o tratamento.

Tendo em vista o exposto, o tratamento de dados realizado pelo empregador será legítimo e legal quando atender a uma finalidade legítima. A mesma deverá ser informada ao empregado anteriormente ao início das operações envolvendo suas informações pessoais, de modo que nunca deverá ser desvirtuada. Caso seja alterada, ainda que sem alterar seu cerne, deve-se informar o titular novamente.

O inciso II do artigo 6º, por outro lado, elucida o princípio da adequação “[...] compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;” (BRASIL, 2018a). Rony Vainzof (2020) o conecta com o princípio da finalidade, de forma que este só poderá ser integralmente garantido quando houver sintonia entre o fim previamente informado ao titular e o tratamento.

Em outra visão, Silvano Flumignan e Wévertton Flumignan (2020) asseveram que, caso o tratamento não esteja coadunando com a finalidade informada ao titular, o princípio da adequação não será atendido. Os autores aduzem ainda que o princípio da adequação expõe um contexto mais objetivo da finalidade.

No que se refere ao princípio da necessidade, o mesmo encontra-se explicitado no inciso III do artigo 6º da LGPD. Bellizze Oliveira e Lopes (2020) anunciam que o princípio da necessidade possui outras manifestações ao longo da LGPD: no parágrafo 1º do artigo 10, no artigo 16 e no inciso VI do artigo 18. Clarificam que o mesmo impõe que os dados sejam coletados e tratados em quantidade mínima necessária para que haja efetivação do princípio da finalidade, de sorte que a eliminação dos dados será imposta caso o titular requeira ou se o tratamento acabar (tiver atingido sua finalidade), sendo assim, os dados não seriam mais necessários.

Danilo Doneda (2011) relaciona o princípio da necessidade à indispensabilidade dos dados para que o tratamento atinja sua finalidade. Atribui-se seu surgimento à doutrina alemã, de modo que explicita uma preferência pelo não tratamento de dados, uma vez que o acesso aos dados, por si só, denota certo acesso à intimidade do indivíduo, de maneira que quanto menos os utilizar, maiores serão as garantias de privacidade. Isso ocorre, pois o princípio da necessidade determina que o tratamento seja feito apenas quando não restar alternativa para que a finalidade das operações que envolvem informações pessoais seja atingida. O autor

explica ainda que esse princípio passou a ter maior importância com a eclosão de técnicas alternativas ao tratamento, como no caso de tornar os dados anônimos, retirando qualquer referência aos titulares.

Silvano Flumignan e Wévertton Flumignan (2020) atribuem duas facetas para o princípio da necessidade. A primeira está relacionada às responsabilidades de quem coleta e trata os dados, já que o mesmo deverá exercer as operações envolvendo dados pessoais com maior cautela, já que quanto mais tratar, maiores serão suas responsabilidades, devendo-se ater ao mínimo necessário para a finalidade desejada. O segundo aspecto está relacionado à obrigação de tratar-se apenas o imprescindível para que a finalidade prévia seja alcançada, de maneira que o não acatamento desta faceta acarretaria em abuso de direito.

Rony Vainzof (2020, p. 136) explica que o princípio da necessidade é denominado, no GDPR, pelos princípios da minimização de dados e limitação da conservação. Destarte, os dados serão tratados em quantidades mínimas necessárias e armazenados no menor decorrer de tempo necessário. O autor ainda assevera que no caso brasileiro, o princípio da necessidade propõe uma mudança de cultura gigantesca, já que o país não possui tradição de proteção de dados, sendo comum a adoção de “procedimentos, por ausência de percepção dos riscos, comodidade e custos envolvidos, de coleta massiva de dados pessoais para depois se pensar nos possíveis usos [...]”.

No tocante ao princípio da minimização de dados previsto no GDPR, o STJ já proferiu acórdão que o elenca:

Destaque-se que o art. 5º daquele documento (GDPR) consagra, entre os princípios fundamentais relativos aos dados pessoais, que a recolha dos dados somente poderá existir com fins específicos, além de estabelecer a minimização dos dados (apenas aquilo que for estritamente necessário), sempre para um fim concreto, além de estabelecer que referido processo seja transparente, leal e lícito. (BRASIL, 2017b)

Portanto, o empregador deverá realizar o tratamento de dados de seus empregados de maneira a empenhar o mínimo de tempo e quantidade de dados, utilizando apenas aqueles imprescindíveis para completar o fim previamente proposto. Logo, caso os dados tenham atingido sua finalidade inicial ou tenham sido coletados em excesso, deverão ser excluídos, ou o empregador estará cometendo abuso de direito.

5.2.2.3 Livre Acesso

O inciso IV aduz o princípio do livre acesso (BRASIL, 2018a). Ana Sanden (2014), em análise baseada na legislação europeia sobre a temática, inclui o princípio do livre acesso como um dos principais fundamentos dos direitos garantidos ao titular nas normas protecionistas de dados. Cita ainda alguns direitos, de rol exemplificativo, atrelados a esse princípio: de apagar, retificar, corrigir informações; de ser informado; de oposição. Assim, são garantidos meios de controle do titular sobre suas informações pessoais após o início do tratamento de dados.

Selma Carloto (2021) refere-se ao princípio do livre acesso como garantia para que o titular dos dados possa corrigir informações que possam ocasionar algum malefício. Define ainda o princípio como o direito a ter conhecimento sobre o tratamento de dados e seus métodos e prazos, de modo simplificado e gratuito. Danilo Doneda (2011) entende que o princípio do livre acesso como um requisito e instrumento imprescindível para que os demais princípios sejam exequíveis.

Wévertton Flumignan e Silvano Flumignan (2020) focam no livre acesso como um dever, uma regra oriunda do próprio princípio da boa-fé e da obrigação de informar o titular dos dados. Bellizze Oliveira e Lopes (2020) asseguram que o princípio do livre acesso está estampado no caput do artigo 9º da LGPD, e ainda nos artigos 18, 19, 20, de modo subentendido, haja vista que estes últimos preveem modos de alcance do titular a seus dados.

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: 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 e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador; 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. (BRASIL, 2018a)

Sendo assim, o princípio do livre acesso garante que o trabalhador tenha acesso sobre seus dados coletados e tratados pelo empregador, tendo direito à ciência dos sujeitos envolvidos no tratamento de suas informações, bem como das técnicas utilizadas. Além disso, assegura controle sobre os dados, de modo que o titular pode solicitar revisão e atualização de dados, retificação, exclusão, inclusão, dentre outras possibilidades.

5.2.2.4 Qualidade dos Dados

Já o princípio da qualidade dos dados é expresso pelo inciso V: “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” (BRASIL, 2018a). Flumignan e Flumignan (2020, p. 131) frisam que o princípio estabelece a obrigação de constante verificação da correta execução de operações envolvendo os dados, dos dados em si e dos protocolos e mecanismos de segurança. Todavia, apontam uma situação excepcional: “A necessidade de atualização somente não ocorrerá em situações em que é proibido a atualização unilateral, como ocorre em áreas sensíveis como a da saúde do usuário”.

Marco Aurélio Bellizze Oliveira e Isabela M. Pereira Lopes (2020) informam que o princípio da qualidade dos dados impõe a clareza, exatidão, objetividade e atualização às informações pessoais. Os autores ainda certificam que o princípio está intimamente interligado com a transparência e o livre acesso, tendo como seu cerne no inciso II do artigo 18 da LGPD, supracitado.

Portanto, o empregador sempre deverá prezar para que as informações pessoais de seus empregados sejam as mais claras e concisas possíveis. Logo, deverá sempre buscar a objetividade e atualização desde a coleta até a exclusão dos dados pessoais.

5.2.2.5 Transparência

O princípio da transparência, contido no inciso VI do artigo 6º da LGPD (BRASIL, 2018a) assegura o alcance facilitado do titular sobre o progresso do tratamento de seus dados pessoais, bem como os agentes envolvidos. Patrícia Peck Pinheiro (2021, p. 10) rememora que a transparência é a “fiel da balança” responsável pela repactuação dos compromissos das instituições da sociedade digital com os direitos fundamentais erigidos após a Declaração Universal de Direitos Humanos de 1948, de modo que estaria presente em todas as legislações protetivas de dados pessoais.

Wévertton Flumignan e Silvano Flumignan (2020) evidenciam que o princípio da transparência já era consagrado pelo artigo 7º do Marco Civil da Internet, sendo relacionado ao direito à informação. Entendem também que a transparência garante o policiamento feito pelo titular e órgãos fiscalizadores sobre as operações envolvendo dados.

Selma Carloto (2021) admite que o controle conferido ao titular, pelo princípio da transparência, garante que o mesmo tenha ciência a respeito de todos os tratamentos, de modo independente da base legal de tratamento utilizada. Rony Vainzof (2020) entende que a transparência possibilita a fiscalização sobre o caráter de segurança, legitimidade, legalidade, propósito, entre outros envolvidos com o tratamento, de maneira a melhor orientar a tomada de decisões do titular. O autor também defende que a transparência será maior conforme maior for o poder do tratamento de dados pessoais.

Larissa Matos (2020) identifica outros pontos, inseridos na LGPD, nos quais são feitas referências ou explicações ao princípio da transparência. São eles: o parágrafo 2º do artigo 10; parágrafo 1º do artigo 20; *caput* e parágrafo 1º do artigo 41 e o artigo 48. Em relação a este último, entende-se que o princípio da transparência impõe para aquele que realizar o tratamento de dados, que comunique tanto o titular quanto a autoridade nacional de proteção de dados caso haja algum incidente que ponha em risco ou acarrete danos à pessoa a quem os dados se referem.

Em torno do apresentado, pode-se inferir que o princípio da transparência possui dois aspectos. Primeiro, impõe que o empregador tenha uma conduta informativa a seu empregado sobre o tratamento dos seus dados. Segundo, garante ao titular dos dados o acesso a informações ligadas às operações realizadas sobre seus dados, desde técnicas, etapas, e pessoas envolvidas.

5.2.2.6 Segurança

O inciso VII do artigo 6º atribui à segurança o caráter de princípio (BRASIL, 2018a). Flumignan e Flumignan (2020) sustentam que o princípio da segurança compele aquele que trata os dados a encargos relacionados a mecanismos que impeçam o acesso de terceiros aos dados pessoais do titular, como por exemplo, as invasões de hackers. Os autores ainda citam o artigo 44 da LGPD, que segue abaixo, como parâmetro para a efetivação do princípio da segurança. Por fim, relembram que a LGPD possui um capítulo destinado apenas para a segurança e boas práticas: capítulo VII.

Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:
 I - o modo pelo qual é realizado; II - o resultado e os riscos que razoavelmente dele se esperam; III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado. (BRASIL, 2018a).

Em análise de princípios de normas relativas a dados pessoais como um todo, Danilo Doneda (2011, p. 1148) nomeia esse princípio como da segurança física e lógica. O autor assegura que esse princípio advém do “dever genérico de cuidado”. Entende que seu surgimento é fruto das próprias responsabilidades geradas pelo uso de tecnologias. Finalmente, citam-se duas disposições que devem ser realizadas para atendimento desse princípio: diferente classificação para os indivíduos que realizarem as operações com os dados, de modo a imputar-lhes responsabilização objetiva em caso de danos ou vazamentos; produção de normas com tecnicidade específica para o tratamento de dados e suas tecnologias.

Bellizze Oliveira e Pereira Lopes (2020) aproximam os princípios da segurança, prevenção, responsabilização e prestação de contas. Entende-se que o da segurança garante que o tratamento não será feito de modo ilícito. Apontam também os artigos 33, 46, 47 e 48 da LGPD como consequência daquele princípio, haja vista que estabelecem diretrizes para evitarem-se práticas ilícitas. A título de exemplo, cita-se o artigo 47 da Lei Geral de Proteção de Dados (BRASIL, 2018a): “Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término”.

Ante o exposto, resta claro que o empregador deverá zelar pelo cuidado no manuseio do uso dos dados de seus empregados. Para isso, possui a obrigação de utilizar técnicas que garantam a segurança dos dados, impedindo o acesso não autorizado por terceiros.

5.2.2.7 Prevenção

O inciso VIII do artigo 6º cataloga o princípio da prevenção, que pode ser entendido através do uso de instrumentos para evitar-se danos envolvendo as operações realizadas com os dados pessoais (BRASIL, 2018a). Rony Vainzof (2020) alega que a LGPD busca criar uma cultura de mitigação de riscos no tratamento de dados. Para isso, prevê meios de proteção do dado pessoal durante todas as fases do tratamento: da coleta à exclusão, de maneira que a análise e busca por instrumentos e procedimentos capazes de garantir maior segurança

estejam sempre presentes. Entende-se também que a privacidade encontrada na lei deve ser feita à luz da *Privacy by Design* (PbD).

Ann Cavoukian (2011) explica que a PbD é orientada por sete princípios, esmiuçados a seguir.

A) *Proactive not Reactive; Preventative not Remedial*: dá-se preferência a atitudes, técnicas e procedimentos que evitam danos, a aqueles que buscam reduzi-los após sua ocorrência.

B) *Privacy as Default*: os padrões adotados pela empresa deverão atender à privacidade dos titulares, assim, seja qual for a operação feita, a privacidade será atendida.

C) *Privacy Embedded into Design*: a privacidade deve ser integrada aos sistemas de informática e aos modelos de negócio, sendo uma parte integrante do que pretende ser entregue, sem diminuir as demais funcionalidades e objetivos.

D) *Full Functionality – Positive-Sum, not Zero-Sum*: a PbD deve garantir que todos os objetivos e interesses legítimos sejam alcançados, permitindo funcionalidades integrais e impedindo surgimento de falsas dicotomias, como por exemplo entre privacidade e segurança.

E) *End-to-End Security – Lifecycle Protection*: pretende-se uma privacidade de ponta a ponta, do começo ao fim de todos os tratamentos realizados.

F) *Visibility and Transparency*: todos os interessados podem verificar o andamento das operações, objetivos e projetos, transparência que torna-se ainda um meio que conquistar a confiança: “Lembre-se, confie, mas verifique” (CAVOUKIAN, 2011, p. 4, tradução nossa).

G) *Respect for User Privacy*: PbD deve garantir o respeito à privacidade do titular, através de fortes padrões de privacidade, notificação apropriada, e empoderamento do indivíduo com opções de fácil manuseio para o usuário.

Selma Carloto (2021) relaciona o princípio da prevenção com o da *accountability* previsto no GDPR. Compreende-se que além de obrigar a adoção de precauções em relação ao surgimento de danos aos dados pessoais, também se deve demonstrar a eficácia das medidas tomadas.

Logo, o empregador deverá atuar de modo preventivo, quando do tratamento de dados pessoais de seus empregados. Ou seja, deve agir anteriormente à ocorrência de qualquer dano ao titular dos dados ou às suas próprias informações, tomando as medidas necessárias para que não ocorram.

5.2.2.8 Não discriminação

O penúltimo princípio postulado no artigo 6º (BRASIL, 2018a) é o da não discriminação. Wévertton Flumignan e Silvano Flumignan (2020) aclaram que a não discriminação assegura que os dados não serão usados para fins ilícitos ou para concretizar abusos de direitos contra os próprios titulares.

Sob o que se pretende combater, Rony Vainzof (2020, p. 150) exemplifica:

As práticas de discriminação podem ser as mais comuns, como a negação de um emprego em razão da religião ou doença do titular, até as mais complexas, como o tratamento preditivo de dados genéticos para fins securitários, que conta, diante da sua criticidade, com preocupações regulatórias próprias.

Larissa Matos (2020) rememora que a luta contra a discriminação é diretriz em outros dispositivos normativos. Primeiro, enfoca-se o objetivo fundamental previsto no inciso IV, do artigo 3º da Constituição Federal de 1988, de modo que o bem de todos deve ser feito, eliminando-se preconceitos e discriminações. Ainda destaca-se a Convenção 111 da OIT de 1965, que regula sobre a Discriminação de Emprego e Ocupação.

Todavia, deve-se fazer uma observação importante. Selma Carloto (2021) defende que a discriminação feita para favorecer grupos que são alvo de discriminação ou as minorias, é permitida e não ofende a Lei Geral de Proteção de Dados. Assim, deve-se prezar pelo princípio da isonomia ou igualdade material. Em relação a esta, Alexandre de Moraes (2021, p. 247) defende que a mesma admite a defesa das “desigualdades”, quando for realizada mediante parâmetros objetivos e racionais para que sejam feitas correções que alterem desigualdades pré-concebidas, ou seja, feita mediante um meio adequado e proporcional.

Portanto, ao tratar os dados do empregado, deve-se prezar pelo seu uso de modo igualitário entre todos os indivíduos. Logo, o empregado não pode sofrer qualquer tipo de abordagem diferenciada e discriminatória, em virtude de suas informações pessoais, quando comparada a feita com outros de seus semelhantes.

5.2.2.9 Responsabilização e Prestação de Contas

O último princípio expresso no artigo 6º da LGPD é o da responsabilização e prestação de contas. Flumignan e Flumignan (2020) relacionam esse princípio pela adoção integral das determinações da LGPD, acrescidas da demonstração desse cumprimento como

forma de assegurar a boa-fé daquele que tratar os dados. Como exemplo, cita-se a evidência do uso de sistemas para garantir a segurança dos dados, da adoção de medidas orientadas por consultoria especializada e do treinamento dos empregados.

Maria Marques (2007) demonstra que os mencionados princípios integram também o rol dos princípios, criados pela OCDE (Organização para a Cooperação e Desenvolvimento Econômico), para a governança corporativa. Sendo esta a responsável por guiar empresas nas melhores decisões, estabelecendo medidas práticas, de forma a evitarem-se problemas na administração.

Larissa Matos (2020) recorda que a LGPD também expressa regras de governança e boas práticas nos artigos 50 e 51. Ainda entende que a maior efetivação desse princípio se dá através do artigo 55-A que criou a ANPD (Autoridade Nacional de Proteção de Dados), órgão que integra a presidência da república e tem como objetivo a fiscalização do atendimento dos preceitos da LGPD.

Rony Vainzof (2020) alerta que a elevação da responsabilização e prestação de contas como princípio demonstra a preocupação da LGPD em advertir aqueles que tratam os dados de que eles são incumbidos de garantir a aplicabilidade e respeito integrais aos preceitos da lei, sob pena de serem responsabilizados, sancionados pessoalmente. Por isso, deve-se observar o atendimento dos princípios, em especial à trindade da finalidade, adequação e necessidade, em seguida, a escolha das bases legais de tratamento, bem como a adoção de medidas de segurança e ainda o acompanhamento de todo o ciclo de vida de operações envolvendo os dados, descartando-os ao final.

Logo, o empregador deverá agir de maneira a cumprir com todos os dispositivos e regras elencados pela LGPD. Deve-se atender aos princípios, bases legais, precauções e medidas de segurança, já que no caso de algum dano ao titular empregado, o empregador poderá ser responsabilizado.

5.2.3 Bases legais de tratamento

Em algumas oportunidades neste presente texto, fora mencionado o termo base legal de tratamento. Estas se encontram previstas nos artigos 7º e 11 da LGPD. Este último denota um requisito para o tratamento dos dados pessoais sensíveis, enquanto aquele outro dos dados pessoais. As bases legais podem ser traduzidas como hipóteses autorizativas de tratamento de dados. Ou seja, os dados pessoais só poderão passar por operações quando a situação for enquadrada em uma das opções contidas nos incisos dos artigos 7º e 11 da LGPD.

Para melhor exemplificar, explicitam-se os incisos do artigo 7º:

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. (BRASIL, 2018a)

Caio Lima (2020) assevera que as hipóteses elencadas pelas bases legais de tratamento são taxativas, de maneira que o tratamento não poderá ser realizado quando não enquadrado estritamente dentre as opções do artigo 7º ou 11. Defende-se também que a cumulação de bases de tratamento é legítima, de forma que aquele que realizar as operações envolvendo os dados deve ater-se – obrigatoriamente – às hipóteses taxativas, mas não lhe será imposto que escolha apenas uma delas.

Chiara Teffé e Mario Viola (2020) informam que a possibilidade de reunião de mais de uma das bases legais de tratamento também ocorre no GDPR. Ademais, defendem que as hipóteses elencadas nos artigos 7º e 11 foram feitas de modo generalizado, sem muitas especificações, de maneira que caberá ao Judiciário, Legislativo e à Autoridade Nacional de Proteção de Dados (ANPD) fazer as devidas ampliações e ajustes.

Augusto Marcacini (2020, p. 142-143) utiliza a terminologia “situações autorizantes” para fazer alusão aos incisos dos artigos 7º e 11 da LGPD. Interpreta-se que a aplicação dessas alternativas legais de tratamento é imposta a pessoas jurídicas de direito público e de direito privado. O autor também explica que dentre as hipóteses, há aquelas que solicitam a autorização do titular dos dados, e outras que dispensam tal requisito.

Guilherme Oliveira (2020) elucida que, embora o consentimento possua suas aplicações, ampla importância, e seja extensivamente divulgado, é caracterizado como apenas uma das hipóteses legais de tratamento de dados, não podendo ser o responsável por resumir a LGPD. Selma Carloto e Elaine Guerra (2021) expõem que o tratamento realizado sem a observância das bases legais, ou até mesmo através da escolha errônea de uma opção de tratamento, acarretará o descumprimento da LGPD e possíveis consequências. Exemplifica que, no âmbito do GDPR, pode ser utilizada como precedente do caso brasileiro, o erro na eleição da hipótese autorizativa vem sendo solucionado através de sanções.

Assim, para que o empregador trate os dados pessoais de seus empregados, deverá ater-se às possibilidades dos artigos 7º e 11 da LGPD. Ou seja, é obrigado a escolher uma ou mais das opções presentes nos incisos daqueles artigos, de modo que a escolha errônea da opção, de acordo com a realidade do tratamento, ou ainda a ausência de escolha, invalida as operações sobre os dados, de modo a poder ocasionar sanções geradas pela ANPD.

6 IMPACTOS DA LGPD NO CONTEXTO LABORAL

Apresentado o histórico da proteção de dados até o surgimento da Lei Geral de Proteção de Dados, convém agora analisar esta sob um enfoque temático. O presente capítulo pretende examinar os reflexos da LGPD no contexto do Direito do Trabalho, demonstrando os direitos dos trabalhadores, bem como as obrigações do empregador.

A princípio, almeja-se investigar se existe possibilidade de aplicação da Lei Geral de Proteção de Dados em conjunto com o Direito dos Trabalhadores, sujeitando-se ao contexto laboral. Em seguida, deseja-se demonstrar algumas peculiaridades envolvendo a LGPD sobre os direitos dos trabalhadores.

Para isso, será verificado como a base legal de tratamento do consentimento interage com a proteção de dados dos empregados. Também será crucial a investigação de como deve ser feita a proteção de dados brasileira durante a execução de processos seletivos e análises curriculares, inclusive no que se referem às informações pessoais de estagiários, aprendizes e adolescentes.

Inserindo-se no ramo laboral, ainda será explorada como se dará a convergência ou divergência envolvendo as negociações coletivas e a proteção de dados albergada pela LGPD, inclusive no tocante da prevalência do negociado sobre o legislado. Ademais, considerações serão feitas sobre a confluência entre as organizações de tendência, os direitos dos trabalhadores que nela laboram e a proteção de dados.

Enfim, será observada a interação entre a proteção de dados do empregado público e os princípios e deveres da administração pública, principalmente no que se refere à necessidade de publicitação dos gastos públicos nos portais de transparência. Por fim, será explorada a limitação temporal do tratamento de dados dos trabalhadores e a consequente exclusão dos dados pessoais dos bancos de dados do empregador.

6.1 LGPD e sua aplicabilidade no âmbito laboral

No âmbito europeu, a aplicabilidade do GDPR no âmbito laboral é muito clara. Conforme garante Anrijs Šimkus e Patrick Van Eecke (2020), o artigo 88 da GDPR prevê expressamente a aplicação da lei, bem como a possibilidade dos países membros estipularem normas específicas sobre a proteção de dados nas relações de trabalho. O mencionado dispositivo possui como antecessor o artigo 8 da Diretiva 95/46/EC, que falava sobre o tratamento de categorias especiais de dados.

Contudo, a incidência da LGPD no ramo laboral não é expressa. Por isso, convém examinar como se dá a aplicabilidade da lei brasileira através de seu artigo 3º (2018a): “Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados [...]”. Também é fundamental recapitular o conceito de dado pessoal como sendo aquela informação referente à pessoa física ou natural.

No que se refere aos citados dispositivos normativos, depreende-se que a LGPD é aplicável a todo tratamento de dados pessoais, ou seja, a todas as operações envolvendo informações de pessoas físicas, sendo aquelas realizadas por pessoas jurídicas ou naturais. Isto posto, deve-se analisar o caso sob cinco perspectivas.

Primeiramente, no tocante ao tratamento de dados pessoais realizados por pessoa física ou jurídica, o mesmo ocorre, cotidianamente, no ambiente empresarial e trabalhista. Trata-se de operações ínsitas a todo negócio, no qual o empregador pessoa física ou jurídica utiliza dados pessoais de clientes, e ainda o de seus empregados.

Sobre a intensa operacionalização de dados no ambiente de trabalho, Vicente Vasconcelhos Coni Jr. e Rodolfo Pamplona Filho (2021, p. 24) proferem:

Assim, no sistema brasileiro se há um campo jurídico que será diretamente impactado pela LGPD, trata-se da seara trabalhista, justamente pelo fato de ser a relação de emprego fonte de vasta fertilidade de fornecimento, utilização, transferência e armazenamento de dados pessoais, aplicando-se a todas as empresas, independentemente de seu porte e/ou atividade exercida. Fica realmente difícil imaginar uma relação de emprego na qual não exista tráfego de dados pessoais [...]

Portanto, o primeiro ponto a ser analisado já garante a aplicação da LGPD nas relações de trabalho pelo simples fato de que as operações que envolvem dados pessoais são inerentes à natureza daquela relação.

O segundo aspecto importante a ser analisado, é o das informações que são transacionadas: dados pessoais. Estes são identificados como informações relativas a pessoas físicas. Ocorre que a relação de emprego possui alguns requisitos que a caracteriza, dentre os quais, pode-se destacar um deles: a pessoalidade ou pessoa física. Bezerra Leite (2021a) entende que a pessoalidade refere-se à relação *intuitu personae* do empregado, de maneira que este será representado sempre por uma mesma pessoa natural. Vólia Bomfim Cassar (2018) elucida que o contrato de trabalho é efetuado sempre pelo mesmo empregado, uma vez que esse negócio jurídico é intransmissível.

Destarte, a relação de emprego também estará amparada pela LGPD, tendo em vista que o empregado sempre será pessoa física e o empregador sempre deverá realizar operações com suas informações pessoais.

Além disso, a terceira circunstância destacada, consoante entendimento de Pamplona Filho e Coni Júnior (2020), refere-se à ausência da previsão do Direito do Trabalho e das relações trabalhistas no artigo 4º da LGPD. Este artigo expressa hipóteses que excluem determinadas situações do âmbito de aplicação da Lei Geral de Proteção de Dados, a exemplo de tratamentos realizados para fins exclusivamente particulares e não econômicos e também para fins de segurança nacional (BRASIL, 2018a).

Por consequência, a proteção de dados pessoais também será garantida para as relações trabalhistas e o Direito do Trabalho por ausência de exclusão legal desse vínculo e área jurídica, vide artigo 4º da LGPD.

Ademais, o quarto item a ser considerado é o relativo à possibilidade de adotar o GDPR como fonte supletiva de direito comparado para a LGPD, por força do caput do artigo 8º da Consolidação das Leis do Trabalho (BRASIL, 1943). Luciano Martinez (2018) explica que aquele artigo garante às autoridades administrativas e judiciárias que, na falta de norma advinda de lei ou contrato, poderão ser utilizadas técnicas integrativas de norma como a heterointegração, na qual está inserido o uso do direito comparado. Salienta-se ainda que as normas estrangeiras a serem utilizadas não poderão prejudicar o interesse público. Assim, por previsão na CLT, o GDPR poderá ser utilizado como base de direito comparado pela LGPD. Como aquele dispositivo normativo prevê sua aplicação nas relações laborais, por análise supletiva, a LGPD também poderá.

Por fim, é válido também citar as considerações de Carolina Assunção e Luiz Koury (2021) que acrescentam o último aspecto a ser considerado. Os autores entendem que há consonância entre os princípios expostos na LGPD com os ligados ao Direito do Trabalho. Citam como exemplo os princípios da não discriminação e da boa-fé.

Logo, a proteção de dados pessoais proporcionada pela LGPD, bem como os dispositivos normativos desta lei devem ser aplicadas ao ambiente laboral. Isto ocorre haja vista que as transações de dados pessoais são cotidianas nesta relação jurídica, também pelo fato de a pessoalidade e a presença da pessoa natural ser requisito obrigatório da relação de empregado, mas também pelo fato de a relação laboral e o Direito do Trabalho não estarem previstos como hipóteses de não aplicabilidade da LGPD, ainda porque a interpretação supletiva da LGPD baseada no GDPR permite e, por fim, pela compatibilização principiológica entre a proteção de dados da LGPD e o Direito do Trabalho.

6.2 Consentimento e a proteção de dados dos trabalhadores

A primeira base legal de tratamento de dados elencada pelo artigo 7º da LGPD é o consentimento. Ocorre que o consentimento possui particularidades que devem ser analisadas com o devido cuidado quando de seu uso no ambiente laboral.

O Direito do Trabalho possui um princípio mestre que o guia: proteção ao trabalhador. A relação entre trabalhador e a empresa, por si só, é desigual, já que há uma dependência econômica daquele em detrimento desta. Américo Plá Rodriguez (2000) explica que o princípio da proteção ao trabalhador busca igualar essa relação através de uma proteção jurídica favorável ao trabalhador, de maneira a implementar igualdade material.

Luciano Martinez (2020) faz uma tripartição do princípio da proteção ao trabalhador em: princípio da aplicação da fonte jurídica mais favorável, princípio da manutenção da condição mais benéfica, princípio da avaliação *in dubio pro operario*. No tocante à primeira dimensão, o autor entende que havendo mais de uma norma (leis, sentenças normativas, contratos de trabalho, entre outros) possíveis de serem aplicadas, deve-se atender àquela que for mais benéfica ao trabalhador.

Bezerra Leite (2021a) entende o subprincípio da cláusula ou condição mais benéfica como uma espécie de direito adquirido, haja vista que haverá permanência da condição mais favorável ao trabalhador quando do surgimento de outra sobre a mesma temática. Assim, se surgir condição mais benéfica, ela será adquirida, mas se surgir uma maléfica, esta não será aplicada. Por fim, Vólia Bomfim Cassar (2018) assevera que o *in dubio pro misero* ou *in dubio pro operario* garante a aplicação da interpretação mais favorável ao trabalhador quando surgir dúvida razoável sobre o assunto discutido.

Ocorre que o princípio da proteção ao trabalhador pode deslegitimar o uso do consentimento nas relações de trabalho, mesmo que ele seja, na visão de Patrícia Peck Pinheiro (2021, p. 18), a “linha mestra” para o tratamento de dados. A justificativa reside no fato de o princípio da proteção existir por uma desigualdade na relação trabalhista. Ana Frazão expõe que a GDPR explicita sua preocupação quando do uso de consentimento em situações assimétricas, motivo pelo qual a LGPD – conquanto não tenha previsão expressa – também deve prezar pela mesma precaução.

Para o melhor entendimento das problemáticas envolvendo o uso do consentimento como justificativa legal do tratamento em situações desiguais, como a do âmbito laboral, deve-se remeter à conceituação do consentimento. Assim, importa destacar alguns dispositivos contidos na LGPD sobre o consentimento:

Art. 5º Para os fins desta Lei, considera-se: [...] XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada; [...]

Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: [...] § 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

Analisando os excertos citados em conjunto com o Código Civil, Bruno Bioni (2021, p. 183-189) destaca as “adjetivações” do consentimento: informado, livre, inequívoco e finalidade determinada, específico e expresso. Para o presente estudo, destaca-se a classificação do consentimento como “livre”, vez que o autor considera de suma importância o exame do nível de assimetria de poderes. Quanto maior a assimetria, menor será o livre-arbítrio de um e maior o poder de barganha do outro, de maneira a tornar o consentimento como “não livre”. Para isso, o escritor destaca que a forma de encontrar assimetria e de descaracterizar o “livre” é através da presença de alguma espécie de subordinação.

Em torno do apresentado, salienta-se um dos requisitos da relação de emprego: subordinação. Para Luciano Martinez (2020) a subordinação nasce pela simples determinação de tempo e da maneira que o trabalho deve ser executado, estipulando uma relação de hierarquia na qual o empregador tem o poder de comando. Bomfim Cassar (2018) também chama a subordinação de dependência hierárquica e considera que a mesma surge pelo simples dever de obediência do empregado.

Logo, como o empregado deve atender às ordens de seu empregador, como ele é seu subalterno hierárquico, não terá livre-arbítrio pleno, de forma que o quesito “livre” do consentimento passe a ser altamente questionável. André Nascimento (2006, p. 14) conclui que a negação do consentimento pelo empregado resulta em uma ocasião “especialmente desconfortável”. Sobre essa incerteza da legitimidade do consentimento no âmbito laboral, Ana Sanden (2014, p. 62) tece importantes considerações:

Na situação de emprego, há fundadas razões para duvidar se o consentimento pode ser invocado como fundamento de licitude para o processamento. Primeiro porque o empregado ou o candidato ao emprego está frequentemente numa posição ou situação em que não lhe é possível dar livremente seu consentimento. Por estar em situação de subordinação na

relação empregatícia, ele pode se ver em dificuldade ou mesmo impossibilitado de recusar, retirar ou modificar seu consentimento pelo medo de perder uma eventual promoção, de ser de algum modo prejudicado ou até de perder o emprego. Ainda, embora a subordinação desempenhe papel central na avaliação da liberdade do consentimento no contexto do emprego, outros elementos podem também exercer influência na decisão do empregado, como os de ordem financeira, emocional ou prática.

Iuri Pinheiro e Vólia Bomfim (2020) entendem que o uso do consentimento como legitimador do tratamento de dados é dúbio. Citam possíveis casos em que a permanência do empregado era dependente de seu consentimento, de maneira que sua negação poderia resultar em sua demissão. Ainda aduzem que o desequilíbrio inerente à relação de trabalho e a dependência econômica do empregador trazem incerteza se o consentimento fora realmente uma opção ao trabalhador, ou uma espécie de temor reverencial ou de imposição.

Em torno do surgimento de toda a dúvida no uso do consentimento, emerge o poder da aplicabilidade do princípio da proteção ao trabalhador. Recordar-se que sua aceção *in dubio pro operario* garante que, quando do surgimento de dúvida razoável, como no caso do uso do consentimento no âmbito laboral, deve-se adotar aquela interpretação mais favorável ao trabalhador. Consequentemente, o uso do consentimento nas relações de trabalho, encontra sua invalidade e deslegitimação através do princípio da proteção ao trabalhador.

Interessa também analisar como o consentimento é utilizado no ambiente protetivo de dados europeu. O GDPR possui como um de seus componentes os “*Recitals*” ou “*Considerandos*” que são utilizados para clarificar e complementar os dizeres contidos nos artigos daquele regulamento. Dentre eles, salienta-se o *Recital 43*:

A fim de assegurar que o consentimento fora dado de forma livre, não deverá fornecer uma hipótese legal válida de tratamento de dados pessoais em um caso específico onde há um claro desequilíbrio entre o titular e o responsável pelo tratamento de dados. [...]. (EUROPEAN UNION, 2018, tradução nossa)

Assim, o próprio regulamento europeu entende como ilegítimo, de maneira expressa, o consentimento naquelas situações em que haja desequilíbrio de poderes, como no caso da relação de trabalho. Interessante também a análise sobre o parecer emitido pelo Grupo de Trabalho de Proteção de Dados do Artigo 29 – GT 29 (*Article 29 Data Protection Working Party 29 – WP 29*), sendo este um órgão consultivo criado pelo artigo 29 da Diretiva 95/46/CE.

Em 2011, o GT 29 emitiu o parecer n°15, no qual fez comentários sobre a definição de consentimento. No documento, há entendimentos que coadunam com a problematização da adjetivação livre em torno do consentimento no âmbito laboral:

O consentimento apenas será válido se a pessoa em causa puder exercer uma verdadeira escolha e não existir nenhum risco de fraude, intimidação, coacção ou consequências negativas importantes se o consentimento for recusado. Se as consequências do consentimento comprometerem a liberdade de escolha da pessoa, o consentimento não será livre. [...]

Um exemplo disto é o caso em que a pessoa em causa está sob a influência do responsável pelo tratamento dos dados, como no caso de um vínculo laboral. (UNIÃO EUROPEIA, 2011, p. 14)

Embora o supracitado parecer tenha sido feito para a Diretiva 95/46/CE, sua aplicação também é válida para a GDPR e também, possui alta probabilidade de ser aplicada, por interpretação supletiva, na LGPD. Lee A. Bygrave e Luca Tosoni (2020) asseveram que o parecer está relacionado às situações em que há assimetria de poder, como a relação de emprego. Nesta, o consentimento deverá ser analisado com maiores cuidados, de maneira que há uma presunção de que o consentimento não possui a adjetivação necessária “livre”.

Embora haja concordância com esse entendimento, Vólia Bomfim e Iuri Pinheiro (2020) observam uma exceção a essa presunção do consentimento não livre na seara trabalhista. Defende-se, com fulcro no parágrafo único do artigo 444 da CLT, que a questão torna-se menos conturbada quando tratar-se os dados de trabalhadores hipersuficientes (aqueles com nível superior completo e com percepção salarial igual ou superior ao dobro do limite máximo dos benefícios do Regime Geral de Previdência Social). Todavia, os autores entendem que, para a mitigação de riscos ao empregado e empregador, como uma medida de *compliance*, deve-se evitar o uso do consentimento como justificativa legal para o tratamento de dados pessoais nas relações trabalhistas.

Em torno de todo o apresentado, pode-se considerar que o uso do consentimento como base legal de tratamento nas relações de trabalho deve ser mitigado. O princípio fulcral do Direito do Trabalho: proteção ao trabalhador, especialmente em sua acepção *in dubio pro operario*, e também a subordinação inerente à relação de emprego põem em cheque a adjetivação “livre” do consentimento, criando uma presunção de invalidade do consentimento para o ambiente laboral. Esse entendimento é corroborado pela legislação e doutrina europeias. Logo, o uso do consentimento deverá ser evitado e utilizado como última alternativa a ser escolhida como base legal de tratamento nas relações trabalhistas.

6.3 Análises curriculares e a proteção de dados

Faz parte da rotina empresarial e trabalhista a circulação de currículos, de maneira que estes contenham dados referentes a determinadas pessoas naturais. Por este motivo, tais certidões possuem a proteção da Lei Geral de Proteção de Dados (LGPD). Assim, o presente capítulo analisará como deve ser feita a proteção de dados pessoais de candidatos em processos seletivos quando houver recebimento de currículos, prestando também a devida atenção no caso dos currículos que concorrem a vagas de aprendiz e estagiários.

6.3.1 Processos seletivos: currículos e o tratamento de dados

O cotidiano das empresas é permeado de tomadas de decisões e troca de informações. Com o intuito de angariar novos empregados, são feitos processos seletivos ou recrutadores, através dos quais o empregador tem a oportunidade de analisar diversos candidatos e escolher aqueles que ele considerar como os mais bem preparados para atingir os objetivos almejados pela empresa.

Para realizar essa escolha e ter maior conhecimento sobre as características, formações e experiências dos pretendes à vaga de emprego, são recebidos currículos. Estes são documentos formulados pelos próprios candidatos, de modo a conter as suas informações profissionais que eles entendam como relevantes ou de interesse da empresa à qual pretendem ser contratados.

Como os processos seletivos e o recebimento de currículos pelas empresas têm como objetivo a contratação de novos funcionários, pode-se afirmar que são também a gênese da futura relação de emprego. Por isso, pretende-se analisar como o recebimento e análise de currículos podem ser influenciados pela Lei Geral de Proteção de Dados.

As informações profissionais dos candidatos, que estão contidas nos currículos, são consideradas como dados pessoais do pretendente à vaga. Assim, o recebimento e a análise feita sobre os mesmos são caracterizadas como espécies de operações envolvendo dados. Logo, o tratamento de dados feito deverá ser amparado sob as justificativas legais dos artigos 7º e 11 da LGPD.

Parte da doutrina entende que se deve utilizar a justificativa legal do inciso V do artigo 7º (BRASIL, 2018a). Esse entendimento é corroborado por Selma Carloto (2021, p. 47):

Os dados dos candidatos serão tratados sem consentimento, inicialmente, porque se trata de um procedimento preliminar para a execução do contrato, a pedido do titular, nos termos do artigo 7º, inciso V, da LGPD, mas atingida a finalidade deverão ser descartados. Se o candidato desistir do processo seletivo e assim comunicar, os dados também deverão ser descartados, assim como a partir do momento que não houver mais possibilidade de contratação porque não subsiste a finalidade.

Embora o processo seletivo possa representar um procedimento anterior e necessário para o contrato de trabalho, deve-se ter muita cautela na consideração desse fato para a escolha da base legal de tratamento dos currículos. Podem surgir equívocos sobre a situação dos processos seletivos e o uso da base legal do inciso V do artigo 7º: “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”.

Recorda-se que os princípios da boa-fé e da prevenção impõem ao empregador que haja com boa-fé, demonstrando boas intenções e prudência no tratamento de dados. Em torno do suscitado, imaginam-se cenários de processos seletivos com muitos candidatos por vaga. Podem-se exemplificar dois deles: 3 (três) vagas disponíveis para 60 (sessenta) candidatos (5% de possibilidade de contratação de cada candidato) 0 ou 5 (cinco) vagas para 2000 (dois mil) candidatos (0,5%).

Nesses eventos, o número de candidatos é muito superior ao número de vagas. Logo, a quantidade de candidatos que não serão selecionados, será expressivamente maior que o de contratados: no primeiro caso, 57 (cinquenta e sete) não recrutados e 3 (três) contratados; no segundo exemplo, 5 (cinco) e 1.995 (um mil novecentos e noventa e cinco).

Nestes aspectos, destaca-se o *animus contrahendi* ou intenção de contratar, entendido por Maurício Godinho Delgado (2019, p. 347-348) como “[...] a intenção do prestador de se vincular (ou não) a título oneroso e empregatício: inexistindo essa intenção, não há o plano subjetivo do elemento fático-jurídico da onerosidade”. Essa intenção de contratação será ausente para uma gigantesca maioria de candidatos.

Posto isso, ainda que se entenda que as negociações preliminares de um contrato, nas palavras de Vólia Cassar (2018), não vinculem e nem obriguem a assinatura do futuro contrato, parece pouco precavida a utilização da base autorizativa do inciso V para os processos seletivos. Parece estremecer a boa-fé a utilização de uma base legal que pauta-se em um futuro contrato que, no âmbito das possibilidades em um processo seletivo muito concorrido possui, nos exemplos citados, 5% ou 0,5% de ocorrer.

Afinal, põe-se em xeque o nível de legitimidade de uma base legal que propõe “[...] procedimentos preliminares relacionados a contrato” (BRASIL, 2018a), porém expõe operações que realmente serão utilizadas como um procedimento que resultará em um contrato para apenas uma parcela reduzida (0,5 % e 5%, nos exemplos enunciados) dos tratamentos realizados. Em suma, pode-se subentender que a empresa utilizará uma justificativa legal de tratamento que lhe seja muito conveniente e menos trabalhosa quanto a que será proposta abaixo.

Tal cenário seria modificado caso a base dos “procedimentos preliminares” fosse utilizada para as fases finais do processo seletivo. Nesta, as probabilidades de contratação e a intenção do empregador em ter o candidato como seu empregado são maiores. Também é diferente para o caso de uma pessoa física que recebe a confirmação de que será contratada e, então, passa a ver seus dados tratados pela empresa.

Dessarte, não se pretende invalidar o uso dessa base legal para os processos seletivos, porém a boa-fé e a precaução impõem dúvidas à mesma. Por esse motivo, defende-se seu uso cumulado com outra justificativa legal, evitando-se sua utilização como sendo a única.

Para isso, é interessante o uso da primeira hipótese legal de tratamento do artigo 7º: consentimento. Conquanto tenham sido explicadas as problematizações do consentimento na seara laboral, defende-se seu uso no presente caso por três motivações. Primeiro, o contrato de trabalho ainda não está formado, de maneira que não há que se falar em subordinação jurídica entre o candidato e o possível futuro empregador. Segundo, trata-se de um interesse maior do candidato em ter seu currículo analisado, em contrapartida aos interesses legais e de controle interno e burocrático do empregador que são predominantes nas demais situações no âmbito do contrato de emprego. Terceiro, o consentimento – para o presente caso – enquadra-se como a mais legítima, e talvez única, das justificativas legais de tratamento de dados.

Para isso, deve-se também atender a alguns requisitos, especificamente os referentes às adjetivações: informado, livre, inequívoco e finalidade determinada, específico e expreso. No que se referem a estes dois últimos, Bioni (2021, p. 192) explica que a terminologia adotada pela LPGD fora o “específico”, porém será entendido através da utilizada “expreso” contida no GDPR e Marco Civil da Internet. Assim, as concordâncias do titular devem ser especificadas para cada tratamento de dados, não podendo existir um consentimento tácito, sendo também interessante o destaque do mesmo, de maneira a expressar uma concordância inequívoca da pessoa a quem os dados se referem sobre as operações envolvendo suas informações pessoais.

Bruno Bioni (2021) ainda assegura que o aspecto “informado” do consentimento está relacionado à necessidade, imposta àquele que utilizar os dados, em ser transparente e informar o titular sobre as operações, sendo assim um pressuposto para as decisões realizadas pelo titular. Já no que concerne à finalidade, entende-se que o consentimento deverá ser feito com uma finalidade pré-definida que deverá ser aceita pelo titular, sendo necessário um novo aceite no caso de quaisquer alterações que a envolvam.

Por conseguinte, o consentimento deverá ser angariado previamente aos tratamentos realizados. Nele deverão conter as informações relativas às intenções e objetivos daquele que tratar os dados, de maneira que, caso haja mudança de finalidade, a mesma deverá ser informada pelo titular. Ademais, é importante lembrar que o consentimento deve especificar cada tratamento realizado, sendo interessante também seu destaque em um possível contrato de trabalho. Por isso, seriam demonstradas prudência e boa-fé no caso de processos seletivos com diferentes fases, em que fosse colhido consentimento específico em cada uma delas.

Outrossim, recorda-se que o consentimento deverá ser livre, sendo uma verdadeira vontade do titular, ser qualquer influência de pressões. Por fim, alerta-se que o consentimento não poderá ser genérico (deve haver especificações das operações) e também não poderá ser tácito, devendo ser explícito.

Convém pontuar ainda que o processo seletivo e o envio dos currículos poderão ser feitos de dois modos gerais: físico e digital. Em ambos os casos, o não envio do consentimento acarretará na exclusão do currículo ou ainda no seu não recebimento. No tocante ao físico ou presencial, o recebimento do currículo e informações do candidato possui como pressuposto a assinatura do consentimento. Este termo deve ser assinado pelo próprio titular que será atestado através de documentos que o identifiquem civilmente (aconselha-se a juntada de cópia junto ao consentimento) e conterà os tratamentos a serem realizados, bem como suas finalidades. Assim, seriam colhidos três elementos: currículo, consentimento e cópias de documento oficial.

Todavia, o procedimento convencional (físico) acarretará em gastos e maiores burocracias para a empresa. Por isso, é válido que seja adotado o recebimento de currículos através do meio digital (online). O termo de consentimento poderá ser auferido de modo análogo ao presencial: anexado em e-mail juntamente com digitalização de documento e o próprio currículo. Entretanto, para facilitar os procedimentos administrativos, indica-se o uso de formulários online. Estes possibilitam que a manifestação de aceite seja feita através de uma assinatura de consentimento no formulário, não sendo necessário o anexo de outro documento comprovando consentimento.

Do mesmo modo que na forma tradicional, recolhe-se cópia da documentação que autentique que a assinatura esteja realmente feita pelo titular, alguns cuidados devem ser tomados na colheita do consentimento e currículo online. Almeida e Ferreira Filho (2020) orientam que, além da obrigação da colheita do consentimento e do documento digitalizado, seria prudente e demonstraria boa-fé que fossem gravados o e-mail e o *Internet Protocol* (IP) responsáveis pelo envio dos dados pessoais.

Ademais, relembra-se que o uso de justificativas legais do artigo 7º da LGPD é necessário, porém não suficiente. Ou seja, deve-se atenção a outras questões quando no tratamento de dados nos processos seletivos e recebimento de currículos. Como de praxe, os princípios contidos nas LGPD também devem ser respeitados, sob o perigo de deslegitimação de todos os tratamentos realizados.

6.3.2 Estagiários e aprendizes: currículos de crianças e adolescentes

Dentre os inúmeros espécimes de processos seletivos, há dois com nuances que devem ser consideradas no contexto da LGPD: os envolvendo estagiários e também aqueles com aprendizes. A questão torna-se mais delicada, pois essas seleções podem envolver currículos adolescentes. Ocorre que as operações realizadas sobre dados pessoais de crianças e adolescentes possuem regras diferenciadas de acordo com a LGPD.

Recorda-se que o Estatuto da Criança e do Adolescente – ECA (BRASIL, 1990b) conceitua em seu artigo 3º que a criança será aquela pessoa natural com até 12 (doze) anos incompletos e o adolescente aquele entre os 12 (doze) e 18 (dezoito) anos. No que tange ao trabalho de crianças e adolescentes, enfatiza-se os dizeres constitucionais previstos no inciso XXXIII do artigo 7º (BRASIL, 1988): “proibição [...] de qualquer trabalho a menores de dezesesseis anos, salvo na condição de aprendiz, a partir de quatorze anos”. Assim, pode-se também asseverar que o trabalho de crianças é proibido.

A princípio, é importante destacar as definições legais relacionadas aos contratos de aprendizagem e de estágio para entender a possibilidade de existência de adolescentes nessas relações jurídicas.

A Lei nº 11.788 de 2008 elenca em seu artigo 10 a duração da jornada de atividade no estágio:

Art. 10. A jornada de atividade em estágio será definida de comum acordo entre a instituição de ensino, a parte concedente e o aluno estagiário ou seu

representante legal, devendo constar do termo de compromisso ser compatível com as atividades escolares e não ultrapassar:

I – 4 (quatro) horas diárias e 20 (vinte) horas semanais, no caso de estudantes de educação especial e dos anos finais do ensino fundamental, na modalidade profissional de educação de jovens e adultos;

II – 6 (seis) horas diárias e 30 (trinta) horas semanais, no caso de estudantes do ensino superior, da educação profissional de nível médio e do ensino médio regular. (BRASIL, 2008).

Salienta-se que a análise dos incisos I e II demonstra que os estagiários poderão ser estudantes que frequentam os ensinos fundamental ou médio. Assim, pode-se concluir que adolescentes estão entre o rol dos estagiários.

Por outro lado, o artigo 428 da Consolidação das Leis do Trabalho, alterado pela Lei nº 11.180 de 2005 descreve como se dará o contrato de aprendizagem:

Art. 18. Os arts. 428 e 433 da Consolidação das Leis do Trabalho - CLT, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943, passam a vigorar com a seguinte redação:

‘Art. 428. Contrato de aprendizagem é o contrato de trabalho especial, ajustado por escrito e por prazo determinado, em que o empregador se compromete a assegurar ao maior de 14 (quatorze) e menor de 24 (vinte e quatro) anos [...]’ (BRASIL, 2005).

Neste ponto, é explícita a idade dos aprendizes: entre 14 (quatorze) e 24 (vinte e quatro) anos, de maneira que se pode concluir que também poderão ser compostos por adolescentes.

A abordagem do presente texto sobre os processos seletivos de estágio e aprendizagem está sendo feita, pois nessas modalidades a presença de e adolescentes é majoritária. Entretanto, não se descarta a possibilidade de adolescentes que participem de processos seletivos a empregos originalmente destinados a adultos. A própria Consolidação das Leis do Trabalho, por alteração prevista pela Lei nº 10.097 de 2000, que segue abaixo, prevê a possibilidade de trabalho para menores de 18 (dezoito) anos, não sendo permitido o trabalho noturno, insalubre, perigoso (BRASIL, 1988).

Art. 1o Os arts. 402, 403, 428, 429, 430, 431, 432 e 433 da Consolidação das Leis do Trabalho – CLT, aprovada pelo Decreto-Lei no 5.452, de 1o de maio de 1943, passam a vigorar com a seguinte redação:

‘Art. 402. Considera-se menor para os efeitos desta Consolidação o trabalhador de quatorze até dezoito anos.’

[...]

‘Art. 403. É proibido qualquer trabalho a menores de dezesseis anos de idade, salvo na condição de aprendiz, a partir dos quatorze anos.’ (BRASIL, 2000)

Ocorre que o tratamento de dados pessoais de crianças e adolescentes possui regramento que o diferencia dos demais. Conforme se pode verificar nos parágrafos do artigo 14 da LGPD:

Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

§ 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.

§ 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.

[...]

§ 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis. (BRASIL, 2018a)

Pela análise dos parágrafos acima, fica claro que a colheita do currículo de uma criança ou adolescente deveria ser feito com um requisito adicional. Este seria a colheita do consentimento dos pais ou responsáveis legais do jovem candidato. A colheita de dados do jovem (não necessariamente do currículo) sem o consentimento dos responsáveis só seria possível se fosse feito para contatar os responsáveis.

Como verificado acima, os parágrafos do artigo 14 fazem referência apenas às crianças, não citando os adolescentes. Com isso, surgem dúvidas sobre sua aplicação de maneira literal (apenas para casos envolvendo crianças) ou de modo ampliativo (incluindo ainda os adolescentes), uma vez que o *caput* cita tanto as crianças, quanto os adolescentes.

Caio Lima (2020) defende a interpretação literal dos parágrafos do artigo 14 da LGPD. Para fazer suas considerações, o autor analisa o relatório feito pelo relator Deputado Orlando Silva para a Comissão Especial destinada a proferir parecer ao projeto de Lei nº 4060, de 2012 (que culminou na LGPD). Após o exame, depreende-se que a intenção do legislador seria clara no sentido de que a exigência do consentimento dos responsáveis seria apenas para

o caso das crianças, não incluindo os adolescentes, aos quais seria exigido apenas o consentimento comum.

Bruna Jardim (2020) defende a inclusão dos adolescentes no rol de aplicabilidade dos parágrafos do artigo 14 da LGPD. Curiosamente, seu primeiro argumento também se baseia no mesmo parecer de relatoria de Orlando Silva. A autora entende que a ampliação da aplicabilidade não é expressa no parecer, mas tácita. Isso ocorre, pois o parágrafo 2º do artigo 14 da LGPD cita expressamente a aplicação para crianças (não incluindo os adolescentes), porém ao se referir a esse parágrafo, o parecer aduz uma aplicabilidade a crianças e adolescentes: “[...] Ademais, responsáveis que lidem com dados de crianças e adolescentes deverão manter pública informação sobre os tipos de dados coletados, como estes são utilizados e os procedimentos para o exercício dos direitos dos titulares”. (SILVA, 2018, p. 37).

Bruna Jardim (2020) justifica a aplicabilidade ampliada através do direito comparado: o artigo 8º do GDPR expõe proteção diferenciada para o tratamento de dados de crianças e também de adolescentes. Arrazoa também que a ampliação para os adolescentes é a mais compatível com o artigo 226 da Constituição Federal de 1988. Por fim, expõe que o próprio caput do artigo 14, ao dizer que as operações envolvendo dados serão feitas no “melhor interesse” (BRASIL, 2018a) da criança e do adolescente, de maneira que no surgimento de alguma dúvida, seria atendida a interpretação que mais beneficia os adolescentes e crianças. Para o caso em tela, o consentimento dos responsáveis ou pais seria o meio mais protetivo e, portanto, o utilizado pela LGPD.

Em vista da argumentação realizada, entende-se que a interpretação dos parágrafos do artigo 14 da LGPD deve ser feita de maneira a incluir os adolescentes no rol protetivo. Assim, ao realizar um processo seletivo ou receber currículo de criança ou adolescente, a empresa deverá coletar o consentimento específico dos pais ou responsáveis. Caso não fosse feito, o recebimento do currículo deveria ser negado ou os dados descartados. Todavia, podem-se angariar (mas não armazenar) dados do menor apenas como um meio de obter o consentimento do responsável, por apenas uma tentativa. Além disso, o ente recrutador deverá manter públicas as operações que serão realizadas com os dados.

Contudo, da mesma forma que o consentimento convencional deve ter atenção à autenticação do titular, o mesmo deve ocorrer com os pais e responsáveis do menor. Conseqüentemente, deverão ser guardadas cópias de documentos que identifiquem não apenas os pais ou responsáveis como pessoa física, mas também uma prova de sua relação com o menor. Neste ponto, pode-se citar uma certidão de nascimento, uma decisão judicial que torne

a pessoa responsável pelo adolescente ou criança ou ainda a própria carteira de identidade da criança ou adolescente, haja vista que nela contém o nome dos pais. Por interpretação do parágrafo 5º do artigo 14 da LGPD (BRASIL, 2018a), também se entende que é possível a autenticidade da responsabilidade da pessoa que assinar o consentimento, bem como sua relação com o adolescente, através de meios tecnológicos.

6.4 Negociação coletiva e a LGPD

Dentro do cenário trabalhista brasileiro, têm-se os âmbitos dos Direitos Individuais dos Trabalhadores, mas também dos Direitos Coletivos. Dentre estes, destacam-se as negociações coletivas de trabalhadores. Estas são consideradas normas e fontes do direito, sendo fruto de intensa negociação entre representantes dos empregados e dos empregadores.

Com o surgimento da Lei Geral de Proteção de Dados, surge também o questionamento sobre seus impactos no Direito Coletivo do Trabalho. Assim, pretende-se investigar como e, em caso afirmativo, de que modo e sobre quais limites as convenções coletivas poderão regular sobre a proteção de dados pessoais, inclusive no tocante à prevalência do negociado sobre o legislado.

6.4.1 Negociação coletiva e proteção de dados

Como já salientado nos capítulos anteriores, a Lei Geral de Proteção de Dados não possui previsão expressa sobre sua incidência nas relações de trabalho, de modo que também não há qualquer menção sobre as possibilidades de negociação coletiva acerca da proteção de dados dos trabalhadores. Todavia, também foi explicitado que a CLT permite a interpretação supletiva da LGPD. Assim, utilizando o direito comparado contido no GDPR, pode-se concluir que as negociações coletivas poderão contemplar dispositivos relativos à proteção de dados.

Trata-se de garantia exposta pelo item 1 do artigo 88 do GDPR:

1. Os Estados-Membros podem estabelecer, no seu ordenamento jurídico ou em convenções coletivas, normas mais específicas para garantir a defesa dos direitos e liberdades no que respeita ao tratamento de dados pessoais dos trabalhadores no contexto laboral, nomeadamente para efeitos de recrutamento, execução do contrato de trabalho, incluindo o cumprimento das obrigações previstas no ordenamento jurídico ou em convenções coletivas, de gestão, planeamento e organização do trabalho, de igualdade e

diversidade no local de trabalho, de saúde e segurança no trabalho, de proteção dos bens do empregador ou do cliente e para efeitos do exercício e gozo, individual ou coletivo, dos direitos e benefícios relacionados com o emprego, bem como para efeitos de cessação da relação de trabalho. (UNIÃO EUROPEIA, 2016, p. 86).

Ana Sanden (2014, p. 173) explica que o GDPR não só garante a formação de negociações coletivas de trabalhadores sobre proteção de dados, como também permite que a “autorregulamentação” seja feita através de regulamentos da empresa ou de códigos de conduta. Ainda defende que os acordos realizados deverão ser exercidos dentro dos limites legais, não podendo extrapolá-los.

Quanto à validade da negociação coletiva sobre proteção de dados dos trabalhadores, deve-se atentar às regras gerais. Vólia Bomfim Cassar (2018) elucida são quatro os quesitos para sua validade: elaborado na forma escrita; prazo de vigência expresso e com máximo de dois anos; pacto seja feito com autorização de assembleia, respeitado o quórum e; envio de cópia para o Departamento Nacional de Trabalho. Também se recorda que as negociações poderão ser: Convenção Coletiva do Trabalho (CCT) ou Acordo Coletivo do Trabalho (ACT), sendo a primeira um negócio realizado entre sindicatos e o segundo entre sindicato dos trabalhadores e empresa(s).

Quanto aos requisitos e validades, também é interessante analisar o Repertório de Recomendações Práticas da Organização Internacional do Trabalho (RRP-OIT). O documento fora elaborado pela OIT em 1997, após o surgimento da Diretiva 95/46/CE e, conquanto não tenha força vinculante, traz preceitos que nortearão para o bom funcionamento das medidas protetivas de dados dos trabalhadores. Ana Sanden (2014) elucida que o RRP-OIT não almeja ser substituto legal, apenas um direcionador para o desenvolvimento de leis, acordos e convenções coletivas, práticas empresariais e políticas sobre a proteção de dados no meio laboral.

A elaboração do documento coletivo poderá ser feita para estipular parâmetros, códigos e políticas de privacidade internas formuladas por cooperação de empregados e empregadores, conforme suscita o subitem 5.11 do RRP-OIT (INTERNATIONAL LABOR ORGANIZATION, 1997). Os subitens 12.1 e 12.2 “a” a “c” também admitem como obrigatória a presença de representantes dos trabalhadores, de maneira que seriam consultados sobre modificações nos sistemas automatizados de tratamento de dados, também dando ciência sobre qualquer monitoramento eletrônico no ambiente de trabalho e sobre as finalidades e modos de interpretar os dados dos trabalhadores. Assim, a empresa teria suas

obrigações delineadas de maneira mais objetiva e os empregados teriam maior ciência de seus direitos protetivos de dados.

Ana Sanden (2014) explica que o desenvolvimento de documentos que estabelecem boas práticas pela empresa é comum no cenário internacional e proporciona maior transparência nas operações envolvendo os dados. Selma Carloto (2021) assegura também que as normas coletivas auxiliam na própria adaptação da empresa à LGPD, proporcionando maior segurança jurídica tanto para os trabalhadores quanto para os empregadores.

Como exemplos de situações em que procedimentos poderão ser regulados via negociação coletiva de trabalhadores, têm-se as elencadas por Iuri Pinheiro e Vólia Bomfim (2020, p. 71):

A norma coletiva poderia, com relativa facilidade, prever a adoção de um só encarregado para as empresas do grupo, sepultando a discussão doutrinária sobre do tema, ou, dispor sobre direitos do operador, por exemplo.

A rigor, diversas normas coletivas estipulam direitos que, para serem exercidos, demandam tratamento de dados pessoais ou até sensíveis, como a concessão de plano de saúde. Caberá à norma indicar os dados que serão necessários, quem os repassará, quando e por quanto tempo ficarão armazenados.

Logo, as CCTs e ACTs não só poderão criar normas relativas à proteção de dados dos empregados, como também é indicado que assim seja feito. O intuito não reside na criação de novos direitos, mas sim no auxílio à própria implementação da LGPD, garantindo maior transparência e segurança jurídica no tratamento de dados dos trabalhadores.

Em vista do suscitado, entende-se que as negociações coletivas do trabalho que versem sobre a proteção de dados dos trabalhadores são permitidas pela interpretação supletiva da LGPD, utilizando como base o direito comparado contido no GDPR. Além disso, importante salientar que para ser válida, deve atender aos mesmos requisitos das ACTs e CCTs convencionais. Acrescenta-se que não é interessante a criação de direitos que diferem dos preceitos da LGPD. Por outro lado, é válido que sejam criados mecanismos para a correta implantação da proteção de dados dos empregados na empresa, garantindo maior transparência e segurança jurídica para o tratamento de dados.

6.4.2 Artigo 611-A da CLT: prevalência do negociado sobre a LGPD

Ademais, é oportuno o exame se o negociado prevalecerá sobre o legislado, vide artigo 611-A da CLT (BRASIL, 2017a), no tocante à proteção de dados do trabalhador e a

LGPD. Essa discussão decorre do fato de que, embora haja previsão de quais temáticas (expressas nos incisos) serão implicadas pelo artigo mencionado, há o entendimento de que as situações ali descritas enumeram um rol exemplificativo (MARTINEZ, 2018), de maneira que outros assuntos, como a proteção de dados, poderiam – em tese – sofrer as imposições daquele artigo. A presente análise será feita sobre três perspectivas.

Primeiramente, é averiguada a questão sobre a ótica do direito comparado, haja vista que a aplicação da LGPD na seara laboral se dá através da heterointegração. Em estudo solicitado pela Comissão de Liberdades Cívicas, Justiça e Assuntos Internos do Parlamento Europeu, Paul De Hert e Hans Lammerent (2013) asseguram que a liberdade concedida para negociar sobre proteção de dados no âmbito laboral fora feita como forma de complementar o GDPR, não sendo possível o desvirtuamento de seus preceitos.

Em posição semelhante, Anrijs Šimkus e Patrick Van Eecke (2020) explicam que, conquanto o GDPR tenha proporcionado certa discricionariedade para a negociação envolvendo dados pessoais de empregados, as normas criadas não poderão infringir os padrões mínimos contidos no regulamento.

Assim, resta claro que o direito e doutrina comparados previstos no GDPR entendem que se deve garantir liberdade para a negociação coletiva de trabalhadores sobre a temática, contudo a lei protecionista de dados não poderá ser desvirtuada. Se o negociado prevalecer sobre o legislado, a deturpação da LGPD seria certa.

Outro ponto a ser considerado é a respeito da inconstitucionalidade do artigo 611-A da CLT. A temática já possui discussão iniciada no Supremo Tribunal Federal, de modo que o relator Ministro Gilmar Mendes, em despacho, suspendeu os processos trabalhistas sobre o assunto em todo o território nacional, e lembrou também que fora reconhecida repercussão geral sobre a discussão (BRASIL, 2019b).

Maurício Godinho Delgado e Gabriela Neves Delgado (2017) entendem que o artigo 611-A desvirtua tanto o princípio da adequação setorial negociada, quanto à verdadeira função constitucional da negociação coletiva, sendo assim uma ruptura dos padrões protecionistas do trabalhador. Por outro lado, o Ministério Público do Trabalho, emitiu a nota nº 08 (BRASIL, 2017c) e argumentou que o artigo 611-A da, então proposta, reforma trabalhista viola as Convenções da Organização Internacional do Trabalho nº 98 e 154. Estas foram ratificadas pelo Brasil, de forma que possuem caráter supralegal, ou seja, hierarquia normativa superior à CLT (esta possui caráter legal), de maneira que esta última deverá também observar concordância com as Convenções da OIT nº 98 e 154.

Sobre estes dispositivos normativos internacionais, é importante citar o relatório do Comitê de Peritos em Aplicação de Convenções e Recomendações da OIT, que – em análise voltada para o contexto brasileiro no início de 2017 – aduziu: “O comitê relembra que o objetivo principal das Convenções n° 98, 151 e 154 é de promover a negociação coletiva com a visão de aprovar os termos e condições de emprego que são mais favoráveis do que aquelas já estabelecidas pela lei” (INTERNATIONAL LABOR ORGANIZATION, 2017, p. 65, tradução nossa).

Esse entendimento, que deve ser observado na interpretação e aplicação da CLT, corrobora com a compreensão do princípio de vedação ao retrocesso social. Este, na visão de Ana Luíza Lima (2017), é previsto tacitamente pela Constituição Federal de 1988, de maneira que o próprio Supremo Tribunal Federal o reconhece, a exemplo da ADI 4543-MC.

Destarte, é evidente que o artigo 611-A carece de constitucionalidade, por vedação aos princípios da adequação setorial negociada, da vedação ao retrocesso social e ainda por ser considerado como desvirtuador da função constitucional da negociação coletiva.

Por fim, emerge o terceiro ponto a ser investigado: defesa de direitos fundamentais do trabalhador. Mesmo se fosse o artigo 611-A, teoricamente, considerado constitucional, deveria ser observado o caráter de direito fundamental da proteção de dados. Como enunciado em capítulos anteriores, os dados estão intimamente relacionados aos direitos fundamentais previstos constitucionalmente: privacidade e intimidade.

Ocorre que como o artigo 611-A prevê a possibilidade de o negociado infringir o conteúdo da lei, também poderá incorrer em afrontas a direitos fundamentais. Fato este que não pode ocorrer, já que há proteção constitucional a esses princípios. Vólia Bomfim e Iuri Pinheiro (2020) também defendem que a flexibilização dos regramentos envolvendo as operações sobre dados pessoais não é possível por ofensas à privacidade e intimidade.

Ademais, recorda-se que a PEC n° 17/2019 implicará na classificação da proteção de dados como um direito fundamental. Logo, será presumida a depreciação de um direito constitucional fundamental, caso o artigo 611-A da CLT proporcione flexibilização de regras de tratamento de dados pessoais.

Por conseguinte, o negociado não deverá prosperar sobre a LGPD ou quando o assunto for relacionado à proteção de dados pessoais em si, sob o perigo de infringir direitos fundamentais previstos na Constituição Federal: privacidade, intimidade e, futuramente, proteção de dados.

Logo, não haverá aplicação do artigo 611-A (negociado prevalecer sobre o legislado) da CLT quando o assunto for proteção de dados pessoais, haja vista que o direito comparado

não permite essa situação, também por inconstitucionalidade do referido dispositivo legal e ainda por perigo de afronta a direitos fundamentais constitucionais.

6.5 Proteção de dados dos empregados em organizações de tendência

Inúmeras são as espécies e objetivos de empresas presentes no cenário brasileiro. Dentre elas, emerge a figura das organizações de tendência, que são marcadas como empresas que presam por determinada ideologia. Ocorre que, por possuírem características que as diferem das convencionais, dúvidas podem surgir a respeito do tratamento de dados dos trabalhadores que lá laboram, especialmente no tocante aos dados sensíveis. Assim, pretende-se compreender as definições das organizações de tendência, bem como se dará a atuação da proteção de dados de seus empregados.

6.5.1 Raízes históricas e definições

Em uma relação intrínseca, encontram-se os âmbitos trabalhista e empresarial. Isso decorre do fato de que os trabalhadores, em sua maioria, só poderão existir e serão remunerados por um empregador, que poderão ser as empresas. Dentre estas, inúmeras são formas sob as quais se estruturam e são geridas. Sob esse enfoque, surge um gênero de empresas com características peculiares: as organizações de tendência.

Gabriela Gaspar (2020) identifica no cenário alemão de 1920 a necessidade de regulação de empresas que tinham aspectos singulares, principalmente as relacionadas às atividades jornalísticas. Identifica-se a lei dos conselhos da empresa (*Betriebrätegesetz*) como a precursora sobre a matéria, tendo sido proposta diante da preocupação de que as aspirações políticas dos jornalistas tivesse o condão de interferir na gestão dos diretores, de maneira a ocasionar danos à liberdade de imprensa. A autora também acrescenta que tal dispositivo fora ampliado não só para o caso dos jornalistas, como também para todas as organizações carregadoras de tendência. Por fim, elucida que a garantia de respeito aos direitos de tendência do empregador, acarretariam em certas limitações aos empregados.

Luís Winter e Natalia Prigol (2017) entendem que a introdução do trabalhador no ambiente de trabalho empresarial lhe repercute algumas influências, de modo que seus interesses fundamentais devem ser ponderados com os legítimos interesses da empresa, o que pode culminar em restrições ao empregado. Neste contexto, podem surgir empresas que possuem, como sua própria razão de existência, a defesa de algum ideal, seja difundo-o,

cultivando-o ou prestando-lhe serviços. Estas empresas são denominadas como organizações de tendência.

Angel Tena (1994, p. 179) define o conceito das “empresas ideológicas”, como também são conhecidas, através de duas correntes doutrinárias. A concepção ampla ou global, adotada pelo direito alemão e pelo presente artigo, possui como representantes não só os partidos políticos e sindicatos, mas ainda as organizações educacionais, artísticas, de caridade, confessionais, de modo que o prestador de serviços adere a alguma ideologia, uma tendência. Por outro lado, a concepção restrita inclui apenas os partidos políticos e sindicatos (na visão de alguns doutrinadores, também as organizações confessionais), de forma que seriam as criadoras ou apoiadoras de determinado pensamento, sendo esta sua única função de existência.

Juliana Amorim (2020) elenca três requisitos caracterizadores das organizações de tendência: ideologia, pluralismo e livre iniciativa. Para a autora, a conceituação de ideologia pode ser entendida através da defesa de um conjunto de convicções, de maneira que – ainda que minimamente – reproduza distorções da realidade. Sua concretização dá-se pela exteriorização dos ideais através das ações de seus apoiadores. Entretanto, alerta-se que a ideia defendida é fruto de um interesse coletivo, não podendo ser confundida com um interesse isolado que possui apenas a empresa como representante. A difusão da ideologia deve ser coletiva a ponto de ser identificada pelos trabalhadores e até mesmo por terceiros.

José Afonso da Silva (2008) esclarece que a Constituição Federal de 1988 é constituída pelo Estado Democrático de Direito, que possui como um de seus ideais a sociedade plural. Esta é oposta à sociedade monista e opressiva, de maneira que garante a coexistência da pluralidade de grupos sociais e econômicos, ideológicos, entre outros. Assim, a sociedade plural é também uma sociedade de interesses distintos, opostos e pela diversidade de pontos de vista.

Jorge Miyagusuku (2008) identifica o pluralismo como elemento formador das organizações de tendência. Explica que um Estado plural possibilita o surgimento de diferentes ideologias, de modo que as organizações de tendência são fruto do caráter democrático da sociedade, já que facilitam a participação das pessoas nas áreas sociais, políticas, econômicas, sociais através da defesa de uma convicção.

Raquel Tavares dos Reis (2008) assume que o surgimento de uma tendência é fruto da dimensão coletiva da liberdade de pensamento. Isso decorre do fato de que o pluralismo de ideias propicia a formação de grupos defensores de ideologias, grupos interpostos entre o Estado e a pessoa natural.

No tocante ao último elemento caracterizador: livre iniciativa, convém rememorar que a Constituição Federal a elenca tanto como um fundamento da República Federativa do Brasil como um princípio da atividade econômica, conforme citado abaixo:

Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos: [...] IV - os valores sociais do trabalho e da livre iniciativa.

[...]

Art. 170. A ordem econômica, fundada na valorização do trabalho humano e na livre iniciativa, tem por fim assegurar a todos existência digna, conforme os ditames da justiça social, observados os seguintes princípios: [...]. (BRASIL, 1988).

Amorim (2020) relaciona a livre iniciativa como uma das vertentes da liberdade, de modo que garante a atuação econômica sem interferências estatais. Entende-se também que ela é utilizada como um meio de neutralizar a atuação negativa do estado e também como forma de valorização do trabalho. Assim, garante-se ao empregador que dirija seus negócios conforme seus entendimentos e ideologias, sem sofrer restrições por parte do ente estatal. Ou seja, o surgimento das organizações de tendência é uma consequência da livre iniciativa.

Gabriela Gaspar (2015, p. 96) considera ainda como característica das organizações de tendência o fato de serem “[...] realizadoras de direitos fundamentais do seu Titular”. Essa classificação decorre do fato de que essas empresas podem ser o canal para a garantia e defesa de interesses coletivos fundamentais de seus integrantes

Destarte, pode-se inferir que as organizações de tendência possuem seu marco inicial no direito alemão. Além disso, podem ser caracterizadas através das empresas que buscam defender determinada ideologia, que pode ser considerada como a razão de existência daquela pessoa jurídica, como por exemplo, os partidos políticos e sindicatos, mas também organizações confessionais religiosas ou uma loja que venda produtos destinados apenas para pessoas obesas. Essas organizações possuem ainda como requisitos caracterizadores a ideologia, o pluralismo, livre iniciativa, sendo ainda um meio de concretizar direitos fundamentais de seus participantes.

6.5.2 Ideologia e o tratamento de dados sensíveis

Como já exposto, as organizações de tendência baseiam seu funcionamento na defesa de terminada convicção. Ocorre que a defesa de uma ideologia no âmbito laboral pode

ocasionar surgimento de algumas particularidades. Estas podem resultar em imposições e conflitos entre o direito do empregador e de seus empregados, sendo estes últimos passíveis de sofrerem restrições incomuns a quando comparadas a outras da seara trabalhista.

Sobre esta conjuntura, elucida Raquel Tavares dos Reis (2008, p. 100-101):

Se, no momento em que ingressa na organização produtiva – ou em qualquer outra organização, pois a simples ideia de ingresso numa organização implica uma certa compressão dos direitos, liberdades e garantias de que uma pessoa é, enquanto tal, titular, não podendo a vida da organização desenvolver-se sem essa compressão –, o trabalhador não renuncia aos direitos, liberdades e garantias reconhecidos a todas as pessoas só pelo facto de o serem, a celebração do contrato de trabalho supõe necessariamente que esses direitos se sujeitem a certas limitações, significando tal ingresso, podemos dizê-lo, uma renúncia aos modos de exercício de tais direitos que possam colidir com os direitos da entidade empregadora.

Jorge Miyagusuku (2008) adverte que a ideologia defendida pela organização, por ser um direito do empregador, deverá também ser imposta a todos os empregados. A livre iniciativa corrobora não só para a formação, mas também o desenvolvimento das atividades do empregador, de forma que a ideologia deste constituirá também parte do contrato de trabalho. Por isto, restringirá também as liberdades dos empregados.

Assim, as organizações de tendência, como meio de defender seus ideais, poderão exigir-los também de seus empregados, ou até mesmo aos candidatos de emprego.

Acontece que as convicções defendidas por essas empresas estão relacionados a dados sensíveis. Por exemplo, um partido político defende uma opinião política e também pode relacionar-se a filiação de organização filosófica ou política; uma loja cujas vestimentas atendam apenas pessoas obesas interliga-se com informações sobre a saúde da pessoa; uma escola confessional interage com convicções religiosas e ainda sobre filiação a organização religiosa. Todas essas inter-relações são previstas como dados sensíveis no artigo 5º, inciso II da Lei Geral de Proteção de Dados (BRASIL, 2018a).

Para exigir essas informações em processos seletivos das organizações de tendência ou até mesmo como um meio de restringir as atividades dos empregados, devem-se utilizar as bases legais de tratamento previstas no artigo 11 da LGPD. Como a tendência defendida é composta pela livre iniciativa e o pluralismo (princípios constitucionais), ela constitui-se tanto como um direito fundamental do empregador, quanto um meio de exercê-lo. Destarte, a base de dados escolhida, deverá atrelar-se a esse fato, de modo que será a prevista no inciso II, alínea “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)” (BRASIL, 2018a).

O mesmo entendimento é corroborado por Gabriela Gaspar (2020). A autora, porém, alerta que a escolha da justificativa legal de tratamento não basta, de modo que deve haver respeito aos princípios elencados pela LGPD. Dentre estes, destaca o da adequação (harmonia entre a tendência e o tratamento), necessidade (dados mínimos necessários, afastando dados dispensáveis), finalidade (apenas para fins legitimados pela tendência), transparência, não discriminação (o uso dos dados deve ser feito apenas para defesa da convicção, de modo que não poderão ser utilizados com o fim de marginalizar aqueles que não se coadunem com a ideologia pregada).

No tocante ao princípio da necessidade, deve-se frisar um ponto relativo aos empregados das organizações de tendência.

Angel Tena (1994, p. 179-180) explica que a doutrina alemã desenvolveu a denominação “*tendenzträger*” para especificar os trabalhadores cujas funções estão relacionadas à tendência. Também elucida que a doutrina italiana desenvolveu as caracterizações de tarefas de tendência, para referir-se àqueles serviços ligados à finalidade de organização de tendência, e tarefas neutras para àqueles que não tiverem conotação ideológica, ou seja, forem apenas funções burocráticas, técnicas.

Raquel Tavares dos Reis (2008) entende que o dever do trabalhador de adequar-se à ideologia da organização, privando-se de atividades contrárias à convicção defendida, é inerente ao contrato de trabalho. Porém, compreende que a submissão à ideologia deve ser feita apenas para as funções de tendência, ou seja, às relacionadas ao pensamento protegido. Por outro lado, as funções consideradas como neutras, já que não se relacionam à tendência, não sofrem essa influência.

Juliana Amorim (2020, p. 15) identifica como sendo “portadores de tendência” aqueles cujas funções possuem relevante teor ideológico. Assim, costumam estar relacionados com a própria propagação e difusão dos ideais defendidos pela organização. Gaspar (2015) explica que é através da atividade dos portadores de tendência que a organização atinge sua finalidade e demonstra sua identidade.

Em outras palavras, aqueles empregados, em cujas funções são identificadas a ideologia e o fim da organização, serão considerados como portadores de tendência. Em contrapartida, as tarefas neutras podem ser as mais variadas possíveis dentro da empresa, sendo apenas necessário que suas atribuições não estejam relacionadas com a ideologia defendida.

Recorda-se que o princípio da necessidade contido na LGPD impõe que o tratamento seja feito apenas quando necessário, de modo que influencie apenas os dados indispensáveis. Como os trabalhadores neutros não precisam da ideologia identificadora da organização para que suas atribuições sejam realizadas e, de mesmo modo, a finalidade da organização de tendência não prescinde das funções neutras para ser atingida, então os dados sensíveis dos empregados ou candidato às funções neutras não precisarão ser angariados ou tratados.

Considerações semelhantes são traçadas por Gabriela Gaspar (2020):

Assim, a necessária conexão entre limitação de direitos e defesa da atividade ideológica da organização proíbe uma indiscriminada extensão das citadas limitações naqueles trabalhadores que desenvolvem funções sem conteúdo ideológico algum, vale dizer, aqueles empregados que realizam as chamadas “tarefas neutras”. Portanto, qualquer restrição ao exercício de seus direitos, através do contrato de trabalho, carece de necessária justificação, tornando-se abusiva e, portanto, plenamente ilegítima.

Do mesmo modo, a coleta de dados sensíveis para os empregados ou candidatos que realizam ou irão realizar tarefas neutras, ou seja, sem conteúdo ideológico algum, se mostraria ilegítima, podendo ser, inclusive, discriminatória, já que careceria de elemento justificador para a coleta desses dados, não podendo ser enquadrada na hipótese o art. 11, II, “d”, da LGPD.

Destarte, além da observância da base legal de tratamento contida no inciso II, alínea “d” do artigo 11 da LGPD, a organização de tendência deve ater-se a outros pontos. Dentre estes se destaca o alinhamento com os princípios da LGPD. Em relação ao princípio da necessidade, deve-se atender a um tratamento que seja realizado apenas aos dados imprescindíveis para que a defesa da ideologia da organização seja atingida.

Para isso, os dados sensíveis só poderão ser tratados quando referirem-se aos empregados ou candidatos das funções portadores de tendência. Como o desempenho dos trabalhadores neutros não são indispensáveis para a finalidade da organização de tendência, seus dados sensíveis não serão legitimamente tratados, já que não são necessários para o exercício regular de direito do empregador em defender e difundir a ideologia de sua organização de tendência.

6.6 Proteção de dados dos empregados públicos

A Administração Pública deve garantir o respeito a alguns princípios instituídos pela Constituição Federal de 1988 e por leis. Por este motivo, atendendo ao princípio da publicidade, também é obrigada a divulgar os gastos realizados pelos seus entes. Neste

cenário, surge a divulgação dos gastos públicos envolvendo a remuneração de empregados públicos, de modo a expor também o nome desses indivíduos (um dado pessoal). Ocorre que o surgimento da LGPD impôs novos regramentos à proteção de dados e à privacidade. Assim, resta a dúvida de como poderia ser feita a ponderação entre a divulgação dos gastos e a garantia da publicidade com a proteção de dados e a privacidade dos empregados públicos.

6.6.1 Princípio da publicidade

A administração pública no Brasil é estruturada e guiada por diversos dispositivos normativos e princípios que possibilitam o cumprimento de suas obrigações e missões constitucionalmente previstas. Dentre os princípios, podem-se citar a supremacia do interesse público e da continuidade dos serviços públicos, dentre outros. Entretanto, os que mais ganham destaque são aqueles evidenciados de maneira expressa no caput do artigo 37 da Constituição Federal de 1988: “legalidade, impessoalidade, moralidade, publicidade e eficiência” (BRASIL, 1988).

No que concerne ao princípio da publicidade, pode ser definido através do inciso V do parágrafo único do artigo 2º da Lei nº 9.784 (Lei dos Atos Administrativos): “divulgação oficial dos atos administrativos, ressalvadas as hipóteses de sigilo previstas na Constituição”. Assim, o princípio da publicidade criou a obrigação para a Administração Pública de divulgar, de ofício, seus atos administrativos, excetuando apenas as hipóteses elencadas na Constituição.

Alexandre Mazza (2021) observa a correlação entre o princípio da publicidade e o da moralidade, de forma que aquele corrobora para a efetivação deste. Também entende que a publicidade engloba dois princípios do Direito Administrativo: transparência (dever da Administração Pública de prestar esclarecimentos a seus cidadãos) e divulgação oficial (Estado deve publicitar, na forma da lei, os atos administrativos por ele praticados).

O princípio da publicidade é um dos meios de assegurar um controle do Estado pela população, impedindo a formação de regimes totalitários. A importância do princípio da publicidade para o Estado Democrático de Direito é explicada por Rafael Oliveira (2013, p. 101-102):

O princípio da publicidade impõe a divulgação e a exteriorização dos atos do Poder Público (art. 37 da CRFB e art. 2.º da Lei 9.784/1999). A visibilidade (transparência) dos atos administrativos guarda estreita relação com o princípio democrático (art. 1.º da CRFB): o povo, único e verdadeiro titular

do poder, deve conhecer os atos dos seus representantes. Quanto maior a transparência pública, maior será o controle social sobre os atos da Administração Pública e das entidades privadas que exercem atividades delegadas ou de relevância pública.

José dos Santos Carvalho Filho (2020) também identifica a publicidade através do inciso XXXIII do artigo 5º da Constituição Federal, que segue transcrito abaixo, e também a Lei de Acesso à Informação (LAI) ou Lei nº 12.527 de 2011. Esta, dentre outras disposições, busca regular o supramencionado inciso constitucional. O autor ainda aduz que a LAI é aplicável a toda administração pública direta ou indireta, desde a União, Estados, Municípios, até suas respectivas autarquias, fundações, empresas públicas e sociedades de economia mista. Ainda entende que a LAI instituiu duas formas de publicidade: ativa e passiva. Esta garante ao cidadão interessado que possa postular sobre informações perante a administração pública, e aquela impõe ao poder público que exteriorize, de ofício, informações sobre sua atuação.

[...]

XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado; (BRASIL, 1988).

No tocante à Lei de Acesso à informação, seu artigo 8º e seus incisos, abaixo transcritos, criaram uma obrigação relativa à publicidade ativa pela administração pública.

Art. 8º É dever dos órgãos e entidades públicas promover, independentemente de requerimentos, a divulgação em local de fácil acesso, no âmbito de suas competências, de informações de interesse coletivo ou geral por eles produzidas ou custodiadas.

§ 1º Na divulgação das informações a que se refere o caput, deverão constar, no mínimo:

I - registro das competências e estrutura organizacional, endereços e telefones das respectivas unidades e horários de atendimento ao público;

II - registros de quaisquer repasses ou transferências de recursos financeiros;

III - registros das despesas;

IV - informações concernentes a procedimentos licitatórios, inclusive os respectivos editais e resultados, bem como a todos os contratos celebrados;

V - dados gerais para o acompanhamento de programas, ações, projetos e obras de órgãos e entidades; e

VI - respostas a perguntas mais frequentes da sociedade. (BRASIL, 2011)

Atualmente, uma das aplicabilidades consequentes deste dispositivo normativo são os portais de transparência que divulgam, mensalmente, a remuneração dos agentes públicos.

6.6.2 Empregados Públicos e o Direito do Trabalho

Os agentes públicos, por outro lado, são as pessoas físicas responsáveis pela execução, desenvolvimento e planejamento das tarefas dos entes estatais. Assim, são as pessoas naturais que realizam funções e possuem cargos na administração pública direta e indireta, de modo que são os meios que externam as vontades estatais.

Maria Sylvia Zanella Di Pietro (2021) explica que pertencem ao rol dos agentes públicos: particulares em colaboração com o Poder Público, servidores público, militares e agentes políticos. Os servidores públicos, por outro lado, dividem-se em servidores estatutários, servidores temporários e empregados públicos. Estes, por sua vez, ocupam cargos públicos e possuem contrato de natureza trabalhista (sujeito à Consolidação das Leis do Trabalho), embora também tenham que observar as disposições para investidura, vencimentos, entre outras questões previstas no Capítulo VII, do Título III, da Constituição Federal de 1988, assim como também aos dizeres da Lei de Acesso à Informação.

Luciano Martinez (2020) explica que os empregados públicos possuem vínculo permanente com seus contratantes, de natureza contratual (leis trabalhistas). Explica que os empregados públicos são divididos em dois grupos (ambos possuem relação jurídica regida pela Consolidação das Leis do Trabalho): servidores públicos celetistas e empregados públicos (em sentido estrito), de maneira que este último labora para as empresas públicas e a aqueles para a Administração Pública Direta, fundacional e autárquica.

Por outro lado, Vólia Cassar Bomfim (2021) também entende que os empregados públicos são regidos pela CLT, porém aduz que laboram perante as sociedades de economia mista e empresas públicas. Recorda que essa classificação os diferencia dos servidores públicos estatutários, que laboram para os demais entes da Administração Pública Direta e Indireta.

Bezerra Leite (2021a) entende que os empregados públicos são também chamados de servidores públicos celetistas, de forma que possuem os mesmos direitos dos empregados celetistas civis convencionais. Porém, adverte que os empregados públicos possuem algumas ressalvas constitucionais, como por exemplo: a vedação de acúmulo de empregos, funções e cargos públicos e que contrato celetista do empregado público só terá validade plena após a aprovação do agente em concurso público.

Em torno das possíveis diferenciações doutrinárias em torno do termo “empregado público”, o presente texto trará suas considerações. Para efeitos deste capítulo, entende-se

como empregado público aquele servidor ou agente público que laborará em sociedades de economia mista e empresas públicas, tendo seu vínculo com a Administração Pública regido pela Consolidação das Leis do Trabalho. Por isso, possuem seus direitos regulados pelo Direito do Trabalho, excetuando-se as ressalvas constitucionais e em contrapartida ao Direito Administrativo que regula os servidores públicos estatutário. Como os empregados públicos possuem contratos regidos pela CLT, eventuais ações judiciais que os envolvam será julgada pela Justiça do Trabalho.

Ocorre que os empregados públicos, como todos os agentes públicos, são influenciados pela Lei de Acesso à Informação. Logo, seus nomes e sua remuneração também são divulgados, de maneira aberta ao público, em portais de transparência dos entes pertencentes à Administração Pública.

Todavia, com o fortalecimento da proteção de dados pessoais imposto pela LGPD, algumas dúvidas surgem no tocante à divulgação da remuneração e nomes dos empregados públicos. Afinal, a vinculação do nome do agente público a sua remuneração demonstram aspectos da privacidade, sendo um dado pessoal do empregado público.

6.6.3 Da razoabilidade e proporcionalidade à necessidade na proteção de dados

Sobre a problemática que envolve a privacidade dos empregados públicos e a divulgação de seus nomes atrelados a sua remuneração em portais da transparência, já existe decisão do Supremo Tribunal Federal (STF) a respeito. Trata-se do Agravo em Recurso Extraordinário (ARE) nº 652.777/SP, cuja ementa segue abaixo:

CONSTITUCIONAL. PUBLICAÇÃO, EM SÍTIO ELETRÔNICO MANTIDO PELO MUNICÍPIO DE SÃO PAULO, DO NOME DE SEUS SERVIDORES E DO VALOR DOS CORRESPONDENTES VENCIMENTOS. LEGITIMIDADE.

1. É legítima a publicação, inclusive em sítio eletrônico mantido pela Administração Pública, dos nomes dos seus servidores e do valor dos correspondentes vencimentos e vantagens pecuniárias.
2. Recurso extraordinário conhecido e provido. (BRASIL, 2015a)

Em vista da ementa apresentada, em 2015, a decisão do STF foi no sentido de que é legítima e legal a divulgação dos nomes de servidores públicos (no qual se inclui o empregado público) com sua respectiva remuneração. Todavia, algumas considerações devem ser feitas. A princípio, observa-se que a decisão exarada pelo STF fora feita antes da vigência da Lei

Geral de Proteção de Dados. Assim, a decisão pode não refletir total consonância com os ditames atuais de proteção de dados pessoais e privacidade.

Ademais, devem-se salientar alguns pontos discutidos pela doutrina. Di Pietro (2021) explica que é esperado o surgimento de conflitos aparentes entre normas que asseguram direitos individuais como intimidade ou liberdade de opinião com um interesse público (como no caso da publicidade das remunerações dos empregados públicos). Para essas situações, a autora defende o uso dos princípios da proporcionalidade, através das regras de necessidade, proporcionalidade (em sentido estrito) e adequação. Por conseguinte, intentar-se-ia o mínimo de restrição dos direitos individuais com o mínimo de gastos possíveis, contemplando a maior proporcionalidade ente o fim da norma de interesse público e as maneiras de implementá-la e agindo ainda de modo adequado.

Gustavo Binenbojm (2009) argumenta que as restrições impostas a direitos fundamentais são comuns, já que a própria Constituição Federal incumbe às legislações a tarefa de definir os limites de tais direitos. Entende ainda que o princípio da unidade da unidade da Constituição garante que haja harmonização, de maneira a garantir que todos os princípios e direitos fundamentais sejam contemplados. Para isso, destaca-se a aplicação da técnica da ponderação que é guiada pelo princípio da proporcionalidade.

No voto do relator do ARE nº 652.777/SP, Ministro Teori Zavascki, restou claro que a decisão fora centrada na defesa do princípio da publicidade e a necessidade de acesso à informação de interesse geral ou coletivo (gasto público envolvendo a remuneração dos empregados públicos). Como forma de demonstrar pretensioso uso da razoabilidade e proporcionalidade, o relator cita que dados como o número do CPF do empregado público ou ainda o local em que mora não são divulgados, de modo que são publicados apenas aqueles que garantam o “[...] necessário modo republicano de administrar o Estado brasileiro” (BRASIL, 2015a, p. 9).

Todavia, entende-se que a decisão não utilizou a técnica da ponderação, norteadas pelos princípios da razoabilidade e proporcionalidade, em sua máxima capacidade. Minimizou-se o entrave envolvendo os riscos à segurança e à privacidade do empregado público, de maneira a lhe impor proteção a seus dados pessoais aquém do necessário e possível.

Isla Monsour (2017) posiciona que a decisão exarada pelo STF no ARE nº 652.777/SP careceu de argumentação. A autora entende que a ponderação entre os princípios da publicidade e privacidade fora incorreta, já que presou por uma incompatibilização entre os princípios, tendendo para a defesa de apenas um deles: a publicidade.

Interessante notar que a aplicabilidade dos princípios da proporcionalidade e razoabilidade encontra semelhança na imposição do princípio da necessidade, elencado pela LGPD e presente em leis protecionistas de dados ao redor de todo o globo. Recordar-se a previsão contida no inciso III do artigo 6º da Lei Geral de Proteção de Dados (BRASIL, 2018a): “III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados”.

Os três princípios convergem para a mesma ideia: atender a uma determinada finalidade (no caso, ao princípio da publicidade), de modo a acarretar o mínimo de prejuízos a outros princípios e direitos (privacidade e proteção de dados pessoais do empregado público). Por conseguinte, caso haja um meio de garantir a publicidade dos gastos públicos (remuneração divulgada) e ainda reduzir (em comparação ao que restou decidido no ARE nº 652.777/SP) a exposição do empregado público, ele deverá ser adotado.

Tendo isso em mente, convém expor dois termos elencados na LGPD: anonimização e pseudonimização de dados. Eles estão previstos, respectivamente, no inciso XI do artigo 5º e parágrafo 3º do artigo 13 da LGPD. De forma resumida, a anonimização de dados pode ser caracterizada como a técnica que elimina, em tese, integralmente as possibilidades de identificação do titular a partir de seus dados pessoais. Por outro lado, a pseudonimização dificulta a identificação da pessoa a quem as informações pessoais se referem, de modo a viabilizar o reconhecimento do titular de modo codificado. Danilo Doneda (2020b) assevera que ambas as técnicas são utilizadas como forma de reduzir os riscos inerentes ao tratamento de dados.

Rony Vainzof (2020, p. 89-90) destaca que o dado pessoal anonimizado não deverá viabilizar o reconhecimento do titular dos dados nem mesmo de modo indireto. Informa também que a LGPD não será aplicável sobre as informações que passarem pelo processo de anonimização. Por fim, enumera os fatores a serem considerados para a caracterização de dados anonimizados: a) a impossibilidade total de identificação do titular; b) anonimização feita através de técnicas razoáveis no momento do tratamento; c) impossibilidade de reversão do processo de anonimização por “meios próprios e esforços razoáveis”; d) será considerado como razoável o esforço analisado através de parâmetros objetivos, como por exemplo, a duração do processo que rever os dados anonimizados para pessoais, alisando também as técnicas e tecnologias utilizadas.

Sobre a impossibilidade de reversão do processo de anonimização, é importante tecer algumas observações. Arvind Narayanan and Vitaly Shmatikov (2010) entendem que o

avanço tecnológico transforma a anonimização perfeita em um mito, já que algoritmos podem revertê-la. Por esse motivo, a LGPD cria os critérios acima elencados, dentre os quais se destacam: o uso de técnicas e esforço razoável, além da duração e gastos envolvidos com o processo de anonimização. Trata-se de uma aplicabilidade tácita do princípio da boa-fé, que busca garantir que, embora haja possibilidades reduzidas de reversão da anonimização, aquele que tratou os dados esforçou-se razoavelmente para que isso não venha a ocorrer.

Bruno Bioni (2020) entende que a pseudonimização na LGPD não fora estruturada de modo tão detalhado quanto no GDPR, uma vez que na lei brasileira houve apenas citação e breve explicação do termo, sem muitas delimitações práticas e estímulos expressos. Todavia, assegura-se que há incentivos tácitos para o uso da pseudonimização como um meio termo entre o dado pessoal e o anonimizado.

O autor avalia ainda que, através do exame dos artigos 7º, inciso IV; 11, inciso II, alínea “c”; 13; e 16, incisos I e IV, e da lógica sistemática da LGPD, subentende-se o incentivo a adoção de medidas redutoras de riscos às operações envolvendo dados. Ademais, ainda que não desvincule totalmente o caráter pessoal dos dados, compreende-se que a pseudonimização poderá não ser revertida por terceiros, além de que, caso uma base de dados pseudonimizados seja invadida, menores serão os riscos quando comparados à base que não utilizou essa técnica (BIONI, 2020).

Evandro Ruiz (2020) entende que a pseudonimização não é um método de anonimização de dados e sim de segurança adicional à proteção de dados, haja vista que não impossibilita a identificação do titular, apenas dificulta. A técnica consiste na substituição de um ou mais dados-chave por algum pseudônimo. Usualmente, a substituição é feita apenas sobre um atributo identificador (como por exemplo, o nome ou foto), mas também pode ser feito através de “quasi-identificador” (RUIZ, 2020, p. 105) que são dados que identificam indiretamente o titular (como o número do CPF ou da CTPS).

O Grupo de Trabalho do Artigo 29 (GT 29) também esclareceu alguns pontos sobre a técnica da pseudonimização de dados através do parecer nº 5 de 2014. Identificaram-se as principais técnicas para substituição do pseudônimo: cifragem com chave secreta; função *hash*; Função *hash* com chave armazenada; cifragem determinística ou função *hash* com chave, com eliminação da chave; utilização de dispositivos de autenticação (*tokens*). Outrossim, foram elucidadas três garantias da pseudonimização: identificação (possibilidade de identificação do titular), possibilidade de ligação (possível interligação simples entre bases de dados ou registros, se utilizarem o mesmo pseudônimo para referir-se a uma mesma pessoa natural); inferência (como é possível a identificação do titular, também serão os ataques de

inferência, que poderão identificar o modelo algorítmico utilizado para a pseudonimização). (UNIÃO EUROPEIA, 2014).

Em torno de todo o apresentado sobre a pseudonimização, podem-se fazer alguns apontamentos. A pseudonimização reduz a possibilidade de identificação do titular, de maneira que garante maior proteção a seus dados pessoais e a sua privacidade. Por esse motivo também não impossibilita o acesso dos legitimados à identificação dos dados pessoais e seus respectivos titulares. Logo, a pseudonimização poderia refletir um meio de garantir maior privacidade aos empregados públicos e ainda garantir a publicidade dos gastos nos portais de transparência. Por outro lado, a adoção da anonimização não seria interessante pelo fato de haver total desvinculação dos gastos expostos com o titular dos dados, impossibilitando assim um incompleto controle sobre os gastos estatais.

Sobre o assunto, discorre Isla Maria Amorim de Souza Mansour (2017):

Neste ponto específico, existe uma sensível diferença entre divulgar o quanto se paga a cada servidor público e qual é o valor recebido a título de remuneração do servidor “X”, pois na primeira opção é possível divulgar a remuneração dos servidores públicos, vinculando ao cargo exercido e individualizando por meio de outros métodos, a exemplo do número da matrícula, na segunda opção divulga-se o salário de determinado indivíduo, invadindo uma informação da esfera da intimidade e privacidade do sujeito.

O trecho supracitado explicita como deve ser feito a ponderação entre a publicidade e a privacidade: garante-se o mínimo de proteção ao empregado público e seus dados pessoais e divulga apenas o dado necessário para efeitos de prestação de contas da administração pública: o valor remuneratório. A autora sugere a adoção de diversas técnicas e exemplifica a substituição do nome pelo número da matrícula, explicitando uma tarefa simples e que garante aumento da privacidade do empregado público, garantindo maior efetivação da proporcionalidade e razoabilidade.

Gabriela Lima e Eduardo Dias (2017) expressam solução semelhante: omitindo o nome do servidor público, mantendo a remuneração acrescida apenas do número de matrícula do empregado público ou suas iniciais ou ainda uma relação de remuneração individualizada por cargo. Os autores entendem que seria uma forma de garantir o interesse público e o controle sobre os gastos estatais (*accountability*) e também assegurar a privacidade e intimidade do empregado público.

As soluções apresentadas acima são realmente muito interessantes em relação aos princípios da razoabilidade e proporcionalidade, sendo mais precisas na ponderação realizada

entre a privacidade e a publicidade quando comparado ao decidido pelo STF no ARE nº 652.777/SP. Todavia, tais artifícios encontram-se incompletos em relação aos padrões de proteção de dados atuais, principalmente no que tange ao princípio da necessidade.

Rememora-se que este impõe que os dados sejam coletados em quantidade mínima necessária para que a finalidade inicialmente determinada seja atingida. No caso em tela, a finalidade é exposta através do acesso e controle da sociedade sobre os gastos da Administração Pública, ou seja, defende-se o princípio da publicidade. Ocorre que a divulgação do nome, ou sua abreviatura, ou número de matrícula são dados pessoais e não estão intrinsecamente ligados à finalidade estipulada, de maneira que para atingir-se a plenitude do princípio da necessidade da LGPD, seria interessante eliminá-los.

Surge neste tópico a aplicabilidade da pseudonimização. O dado pessoal desnecessário para a finalidade de divulgação e controle dos gastos públicos (nome do empregado público, número de inscrição, entre outros) poderá ser substituído por um pseudônimo. Destarte, a privacidade e os dados pessoais do empregado público serão protegidos, sem que haja qualquer prejuízo ao princípio da publicidade e ao controle dos cidadãos sobre os gastos públicos.

Sobre o uso da pseudonimização em portais de transparência como um meio de garantir o correto sopesamento entre os princípios da publicidade e privacidade, podem surgir algumas indagações. Dentre estas, pode ser motivo de preocupação a segurança do processo de anonimização sobre o controle dos gastos públicos e seu possível favorecimento ao crescimento de fraudes e desvio de verbas públicas.

Poder-se-ia discutir que a não divulgação dos nomes seria um agente facilitador para essas ilegalidades. Entretanto, deve-se discordar de tal posicionamento, já que a possibilidade de fraudes também poderia se dar com a sistematização pré-pseudonimização, bastando apenas criação de nomes fictícios para ocasionar o desvio da verba pública.

Ademais, também podem surgir questionamentos acerca da verificabilidade das informações pseudonimizadas, uma vez que a análise do cidadão sobre o gasto poderia estar dificultada pela ausência de nome. Contudo, tal opinião não merece prosperar pelo simples motivo de que qualquer indivíduo tem o direito de solicitar esclarecimentos. Di Pietro (2021) entende que a elucidação da controvérsia pode ser feita com a provocação do Ministério Público (MP) ou dos Tribunais de Contas (TCs), feita por qualquer pessoa natural ou jurídica. Estes entes fiscalizadores e investigativos poderão solicitar ou até mesmo obrigar a Administração Pública a reverter o processo de pseudonimização e assim identificar o titular, possibilitando sua verificação.

Essa ideia é também encontrada ao analisar cenário semelhante: limitação, através das normas e princípios da LGPD, da ampla publicidade em portais da transparência sobre os gastos envolvendo o auxílio emergencial e a divulgação de dados pessoais de seus beneficiários, conforme explica Douglas Araújo (2020, p. 20):

Na esteira desse debate, pode-se concluir que a conduta do governo federal em disponibilizar dados pessoais de brasileiros que receberam auxílio emergencial no Portal da Transparência violou os direitos à privacidade e intimidade dessas pessoas. Primeiro porque os dados constantes em cadastros sociais, como o Cadastro Único, não possuem caráter público. Conforme preleciona o art. 8º do Decreto nº 6.135/2007, que dispõe sobre o Cadastro Único para Programas Sociais do Governo Federal, “os dados de identificação das famílias do CadÚnico são sigilosos e somente poderão ser utilizados para as seguintes finalidades: I - formulação e gestão de políticas públicas; e II - realização de estudos e pesquisas”. Segundo porque inexistente liame entre a disponibilização consciente desses dados no CadÚnico e a intenção que lhe fora atribuída, justificada num suposto viés fiscalizatório que ensejou a “transparência” das informações, diversa do propósito e da finalidade do cadastro

Caso fosse a vontade do governo de fiscalizar e investigar eventuais ilícitos no recebimento desse auxílio, deveria acionar os órgãos de controle (Controladoria-Geral da União, Ministério da Cidadania e Receita Federal) que, individualmente e usando dos instrumentos próprios, buscarão reaver eventuais valores auferidos indevidamente.

Em torno dos argumentos apresentados, resta claro que a divulgação dos nomes dos empregados públicos atrelados a suas remunerações nos portais de transparência não está em total consonância com as noções de proteção de dados e privacidade atuais. Para resolver tal situação, garantir a publicidade aos gastos públicos e ainda agir de maneira proporcional e razoável nessa divulgação, deve-se atender ao princípio da necessidade elencado no artigo 6º da LGPD. Para isso, é interessante que seja adotada a técnica da pseudonimização, de maneira que os nomes dos empregados públicos sejam substituídos por um pseudônimo. Com isso, haveria uma ponderação mais condizente entre os princípios da publicidade e proteção de dados (privacidade e necessidade).

6.7 Limitação do tratamento de dados no âmbito laboral

Para estipular limites ao tratamento de dados do empregado, convém citar um dos princípios elencados no artigo 6º, da Lei Geral de Proteção de Dados, especificamente no seu primeiro inciso, é a finalidade. Esta impõe que o tratamento de dados deve ser realizado

apenas quando tiver um objetivo legítimo, previamente especificado e informado à pessoa a quem os dados se referem.

Verifica-se que tal princípio também detém suma importância para a delimitação do fim do tratamento de dados. Isso ocorre por disposição normativa expressa no artigo 15 da LGPD e a consequência prevista no artigo seguinte:

Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses: I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: (BRASIL, 2018a).

Isto posto, surge o questionamento sobre a limitação temporal do uso de dados pessoais pelo empregador. Nesta conjuntura, paira a dúvida sobre a necessidade de exclusão de dados pessoais do candidato a emprego ou do empregado após o término do contrato de trabalho. Para elucidar tais indagações convém rememorar como o tratamento de dados deve ser feito de maneira a respeitar os dispositivos e princípios da LGPD, devendo também explicitar a escolha de uma ou mais base legal de tratamento.

6.7.1 Fim do tratamento em processos seletivos e guarda de currículos

Como já exposto em capítulo anterior, no caso dos currículos enviados para empresas em processos seletivos, a base legal de tratamento será o consentimento (artigo 7º, inciso I da LGPD), cumulado ou não com a que considera o currículo como procedimento preliminar a execução de contrato (artigo 7º, inciso V da LGPD). Após o fim do processo seletivo, três cenários possíveis podem ser encontrados: exclusão dos currículos ou sua manutenção em banco de dados por reiteração do candidato ou conservação para fins estatísticos.

Com o fim do processo seletivo, sua finalidade estará cessada, de maneira que o tratamento de dados deverá cessar e, conseqüentemente haverá a exclusão dos dados e currículos, conforme garante os artigos 15, inciso I e 16 da LGPD (BRASIL, 2018a). No caso do uso exclusivo (não cumulado com outra hipótese autorizativa de tratamento) do consentimento, caso este seja revogado pelo candidato, também deverá cessar o tratamento e excluído o currículo, vide artigos 8º, parágrafo 5º e 18, inciso V da LGPD (BRASIL, 2018a).

Patrícia Peck Pinheiro (2021) entende que a revogação do consentimento e a consequente exclusão dos dados do titular devem ser feitas de modo expresso, o que denota um aspecto da escolha e liberdade garantidas ao titular. Maurício da Fonseca e Fernanda Nogueira (2020) entendem que, embora a revogação do consentimento seja o suficiente para a interrupção das operações envolvendo dados pessoais, ela não invalida os tratamentos já concretizados.

Outra situação possível é a manutenção dos currículos por pedido reiterado do candidato. Faz parte do dia a dia das empresas, o armazenamento de currículos para convocar determinados candidatos quando do surgimento de vagas disponíveis. Trata-se de uma oportunidade benéfica tanto para a empresa, que terá acesso a novo candidato de forma facilitada e sem os gastos de tempo e dinheiro de um processo seletivo; quanto para o candidato, que ganha nova chance de concorrer a uma vaga.

Nesta última ocasião, é interessante a redefinição da finalidade da manutenção dos dados pessoais (currículos) nas bases de dado da empresa. Para isso, deve-se angariar um novo consentimento, específico e expresso para a finalidade de reanalisar o currículo quando do surgimento de novas oportunidades e vagas de emprego na empresa. Por força do princípio da boa-fé, neste caso é interessante a delimitação de um tempo base para essa última finalidade. Almeida e Ferreira Filho (2020) entendem que a delimitação de 6 (seis) meses é o suficiente para demonstrar precaução da empresa e também para garantir tempo hábil para que o currículo torne-se obsoleto para o candidato, que poderá atualizá-lo.

Também é válido constar no termo de consentimento que o currículo será descartado caso seja realizado um novo processo seletivo que venha a angariar novos currículos. Além disso, após o fim da limitação temporal, os currículos deverão ser excluídos ou então mantidos ou atualizados se assim for requerido pelo candidato titular dos dados.

Finalmente, surge a possibilidade de manutenção dos currículos para fins estatísticos internos da empresa. Esta poderá examinar o processo seletivo que fora realizado, de modo a angariar informações para fins de divulgação e direcionamento de novos processos seletivos ou apenas para averiguação interna.

Neste ponto, seria interessante a adoção da técnica da anonimização dos dados, haja vista que os dados pessoais que identificam os titulares (nome, número de documentos, fotos, entre outros) não seriam mais convenientes, apenas os dados que aqueles para fins estatísticos (idade, formação, entre outros). O caso de dado ser anonimizado já é garantida a sua guarda, mesmo depois de atingida a sua finalidade, vide artigo inciso IV do artigo 16 da LGPD:

Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

[...]

IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados. (BRASIL, 2018a).

Além disso, lembra-se que, por força do caput do artigo 12 da LGPD (BRASIL, 2018a), os dados anonimizados não são considerados como dados pessoais. Logo, não estarão submetidos às exigências legais e principiológicas da Lei Geral de Proteção de Dados. Assim, caso sejam anonimizados, poderão ser mantidos nas bases de dados da empresa sem muitas exigências. Entretanto, deve-se ter atenção para o fato de que o dado anonimizado, conforme garante Selma Carloto (2021), será considerado como dado pessoal caso o processo seja passível de reversão, de maneira a identificar o titular dos dados.

6.7.2 Término do contrato de trabalho

Os empregadores seguem muito preocupados com o descarte dos dados se seus ex-empregados após o fim do contrato de trabalho. Essa inquietação reside no fato de que a Lei Geral de Proteção de Dados impõe o fim do tratamento e a exclusão dos dados pessoais quando alcançada a finalidade previamente estipulada para as operações envolvendo os dados. Ocorre que a exclusão total dos dados do ex-funcionário acarretaria em uma impossibilidade de defesa técnica decente em futuros processos judiciais ou administrativos.

No entanto, uma análise mais cuidadosa da legislação demonstra que a preocupação é infundada. Para obter tal posicionamento, é necessário examinar o caso em tela sob o enfoque das bases legais de tratamento. Realmente, após o término do trabalho a finalidade inicial do tratamento de dados, desenvolvido durante a relação de emprego, atinge seu fim. Todavia, assim como no caso dos currículos, é possível que uma nova finalidade, e outras hipóteses autorizativas de tratamento de dados sejam acolhidas.

Destacam-se duas bases legais de tratamento de dados, previstas no incisos II e VI do artigo 7º da LGPD: “II - para o cumprimento de obrigação legal ou regulatória pelo controlador” e “VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral”. Tais hipóteses autorizativas também são encontradas de forma análoga respectivamente nas alíneas “a” e “d” do artigo 11 da LGPD (BRASIL, 2018a). Assim, caso se tratar do tratamento de dados pessoais, deve-se escolher as bases acima elencadas do artigo 7º e no caso de dados pessoais sensíveis, as do artigo 11.

Como exemplo de cumprimento de obrigação legal, pode-se citar o expresso no Decreto nº 10.410 de 2020, responsável por editar o Regulamento da Previdência Social. O parágrafo 22 do artigo 225, conjunto com o artigo 347 daquele dispositivo normativo, assim assegura:

[...]

§ 22. A empresa que utiliza sistema de processamento eletrônico de dados para o registro de negócios e atividades econômicas, escrituração de livros ou produção de documentos de natureza contábil, fiscal, trabalhista e previdenciária fica obrigada a arquivar e conservar, devidamente certificados, os sistemas e os arquivos, em meio eletrônico ou assemelhado, durante o prazo decadencial de que trata o art. 348, os quais ficarão à disposição da fiscalização.

Art. 348. O direito da seguridade social de apurar e constituir seus créditos extingue-se no prazo de cinco anos, contado: [...]. (BRASIL, 2020)

Através do exame dos dispositivos acima expostos, entende-se que o empregador que utilizar o sistema eletrônico de processamento de dados, possui como obrigação legal de armazenar todos os arquivos relativos a documentos trabalhistas por um prazo de cinco anos. Assim, a empresa poderá manter arquivados os documentos relativos a seu ex-empregado, de acordo com a obrigação legal acima elencada, por cinco anos.

Alerta-se que a obrigação legal citada é apenas um exemplo que, muito provavelmente, será aplicável a muitas empresas. Porém, não exclui outras obrigações legais já existentes. Logo, caso haja alguma lei que preveja a obrigação de manutenção dos dados do ex-empregado por quinze anos, assim deverá fazer a empresa, devendo apenas realizar a documentação necessária para provar tal obrigação legal e escolha de base de tratamento.

O mesmo raciocínio será utilizado no surgimento de nova lei, de forma que a nova imposição legal, caso preveja guarda por tempo maior que o acima explicitado, deverá ser atendida. Se previr tempo inferior, apenas poderá ser atendida se a empresa a escolher como hipótese autorizativa de tratamento ou, se a obrigação supracitada for revogada ou não aplicável ao caso.

No que tange à hipótese de retenção dos dados como garantia do exercício de defesa em futuros processos administrativos, arbitrais ou judiciais, outra sistemática deve ser observada. Como a LGPD possui princípios que obrigam que os dados sejam angariados e utilizados apenas quando necessários, bastando a garantia da finalidade do tratamento, este deverá ser feito sobre quantidade e tempo mínimo possíveis.

No que se relaciona ao tempo necessário para o exercício de direitos em processo, deve-se observar o caso da prescrição trabalhista: bienal e quinquenal, conforme assegura a

Consolidação das Leis do Trabalho, via redação dada pela Reforma Trabalhista: “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.” (BRASIL, 2017a), e da Constituição Federal de 1988, abaixo citada.

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; (BRASIL, 1988)

Assim, em uma análise superficial é possível concluir que a empresa deverá guardar os dados por dois anos (se nenhuma ação do ex-funcionário reclamante for pleiteada) cinco anos (caso a ação seja proposta). Porém, as prescrições trabalhistas possuem muitas possíveis problematizações. Luciano Martinez (2020) explica que a prescrição poderá ser nuclear, também conhecida como total (atingindo todos os atos jurídicos anteriores ao término do prazo prescricional) ou ainda será parcial (impactando apenas parcela dos atos jurídicos). Essa classificação tem grande importância para a LGPD, haja vista que quando da prescrição parcial, o empregador poderá guardar os dados que poderão ser utilizados para defesa daqueles atos que não foram impactados pela prescrição.

Vólia Bomfim e Iuri Pinheiro (2020) citam ainda alguns casos que impactam a prescrição. Primeiro, recordam que a prescrição pode ter causas de suspensão ou interrupção. Para isso, podem-se salientar as hipóteses em que absolutamente ou parcialmente incapazes (não corre a prescrição, conforme artigo 440 da CLT), doenças ocupacionais (vide súmulas 230 do STF e 278 do STJ, a prescrição só iniciará quando da ciência da doença) e ainda no próprio vínculo empregatício, que de acordo com o artigo 11 da CLT, é imprescritível.

Ainda sobre os processos judiciais, é válido ressaltar os cenários envolvendo os recursos e o trânsito em julgado. Se a empresa receber notificação para responder processo judicial movido por ex-empregado, terá o direito de manter os dados do reclamante guardados durante toda a tramitação processual, incluindo as hipóteses de recursos para outras instâncias da Justiça do Trabalho, podendo a eliminação ser postergada até mesmo após o trânsito em julgado.

Para a manutenção dos dados após o trânsito em julgado, devem-se observar os dizeres do artigo 836 da CLT e os artigos 966 a 975 do Código de Processo Civil – CPC. Bezerra

Leite (2021b) informa que os dispositivos contidos no CPC sobre a ação rescisória são todos aplicados ao processo do trabalho, exceto no que se refere à isenção de depósito prévio. No que tange ao prazo de proposição da ação rescisória, cita-se o artigo 975 do CPC:

Art. 975. O direito à rescisão se extingue em 2 (dois) anos contados do trânsito em julgado da última decisão proferida no processo.

§ 1º Prorroga-se até o primeiro dia útil imediatamente subsequente o prazo a que se refere o caput, quando expirar durante férias forenses, recesso, feriados ou em dia em que não houver expediente forense.

§ 2º Se fundada a ação no inciso VII do art. 966, o termo inicial do prazo será a data de descoberta da prova nova, observado o prazo máximo de 5 (cinco) anos, contado do trânsito em julgado da última decisão proferida no processo.

§ 3º Nas hipóteses de simulação ou de colusão das partes, o prazo começa a contar, para o terceiro prejudicado e para o Ministério Público, que não interveio no processo, a partir do momento em que têm ciência da simulação ou da colusão. (BRASIL, 2015).

Examinando o artigo supracitado é possível estabelecer três possíveis prazos, contidos em cada um dos parágrafos de artigo 975, cada um deles relacionados com as possíveis motivações e alegações daquele que desejar rescindir. Não convém analisar todos os parágrafos, apenas aquele que estipula o maior prazo, uma vez que a empresa não tem o condão de prever qual a motivação ou alegação poderá ser feita. Assim, dever ser garantindo tempo hábil para a defesa plena em todas as possibilidades, de modo que para isso ocorrer, basta que seja garantindo o maior tempo previsto em lei.

Ocorre que a previsão do parágrafo 3º não é dada através de um prazo objetivo com delimitação certa. Marcus Gonçalves (2020) explica que os prazos do artigo 975 são decadenciais e que o parágrafo 3º garante ao Ministério Público e ao terceiro interessado que poderão ajuizar ação rescisória, com justificativa em simulação ou colusão das partes, com prazo contado apenas a partir de sua ciência. Como a empresa não pode controlar quando um indivíduo interessado terá ciência desses possíveis fatos, para sua segurança, e para possibilitar a plenitude de defesa, entende-se que os dados pessoais poderão ser armazenados por tempo indeterminado (apenas para os casos em que o processo judicial fora iniciado e, por isso, haja possibilidade de ação rescisória).

Alerta-se que, além da observância dos prazos acima comentados, seria prudente que a empresa procedesse à exclusão dos dados apenas cerca de 1 (um) mês depois de findado prazo, devido à possibilidade de algum atraso da secretaria de vara ou tribunal trabalhista. Ademais, como forma de demonstrar boa-fé e assegurar a segurança dos dados, é interessante também que o ex-empregador faça uso da técnica da pseudonimização sobre os dados do

empregado após o fim do contrato de emprego. Ademais, seria juridicamente seguro, precavido e interessante que o empregador, ao realizar exclusão de dados que o fizesse após contato com o sindicato do empregado, de maneira a exigir do sindicato obreiro algum recibo que atesta que os dados foram excluídos pelas justificações casuísticas e legais nele explicitadas. Caso não houvesse resposta do sindicato ou a mesma fosse negativa, também seria importante que o empregador se munisse de alguma prova da tentativa de contato.

Logo, em torno do apresentado, resta dificultada a estipulação de um prazo temporal que garanta a guarda dos dados pessoais do ex-empregado. Para proceder com o armazenamento, a empresa deverá ater-se às circunstâncias de cada contrato de trabalho, fazendo uso das bases legais de tratamento (com destaque para as relacionadas à obrigação legal e ao exercício de direitos em processo) e tendo ainda muita atenção aos prazos prescricionais.

Conclui-se que a limitação do tratamento de dados após o fim do contrato de trabalho é feita de maneira casuística, não sendo possível a estipulação de uma delimitação temporal e sim circunstancial. Esta se interliga com as prescrições trabalhistas enquanto os processos judiciais, administrativos e arbitrais não se iniciarem, de maneira que se o processo não for iniciado, o prazo será de dois anos. Também é possível afirmar que, nos casos envolvendo possibilidade de surgimento de doença ocupacional manifestável depois de determinado período e também caso em que a ação judicial for iniciada, por possibilitar a ação rescisória, o prazo será indeterminado.

7 CONCLUSÃO

Em torno de todo apresentado ao longo do trabalho pode-se entender que os dados foram inseridos, paulatinamente, no cotidiano da sociedade contemporânea, de modo que são meio de reconhecimento e inserção social. Eles passaram a ser considerados como uma mercadoria, um ativo que é transacionado por compra e venda, e também um instrumento capaz de guiar não apenas ações do mercado, mas ainda influenciar em eleições envolvendo todo um país. Instaura-se assim uma nova fase do mercado capitalista, conhecida como mercantilização digital ou economia digital, na qual os dados são o elemento central.

Ocorre que os dados podem referir-se a informações pessoais de pessoas naturais, de maneira a integrar parte da intimidade e privacidade das pessoas. Ocorre que estes últimos são princípios constitucionais, de maneira que corroboram para que os dados pessoais tenham proteção especial. Todavia, as noções clássicas de privacidade destoam das atuais demandas protetivas dos dados pessoais.

Diante disso, e com inspiração em decisão exarada em 1983 pelo Tribunal Constitucional Alemão, emerge o direito à autodeterminação informativa. Este garante um nível de controle da pessoa natural sobre suas informações pessoais e o tratamento de seus dados. Por isso, o supramencionado direito também é assimilado como uma espécie de evolução, de *upgrade* tanto do direito à privacidade (apesar de não poder ser entendido como seu sinônimo), como também dos direitos de personalidade.

Foram examinados também os precedentes à legislação brasileira de proteção de dados. Inúmeras foram as leis sobre proteção de dados pessoais que regulavam as operações envolvendo-os. Contudo, um novo patamar fora atingido com a aprovação do *General Data Protection Regulation* (GDPR) que fora uma lei geral que instituiu regramentos para o tratamento de dados em torno de todo o continente europeu.

Sucedeu-se que, como o velho continente possui forte influência sobre o comércio mundial, de forma que a criação do GDPR culminou em um efeito dominó no comércio internacional. Isso se deve ao fato de que os países que desejassem manter ou iniciar relações comerciais com os membros da Europa deveriam criar leis protetivas de dados semelhantes ou mais rígidas que o GDPR.

Neste cenário surge a Lei nº 13.709/2018 ou Lei Geral de Proteção de Dados (LGPD), muito semelhante ao GDPR, porém aplicável no Brasil. Ela surge após um grande vazio normativo sobre proteção de dados no país. Anteriormente à sua aprovação, as informações pessoais de pessoas físicas no Brasil eram tuteladas através de leis e institutos esparsos, como

por exemplo, o *habeas data*, alguns pontos no Código de Defesa do Consumidor ou ainda do Marco Civil da Internet.

Embora tenha sido promulgada apenas em 2018, o Projeto de Lei que resultou na LGPD fora iniciado no ano 2012. Logo, o marco normativo internacional que influenciava a LGPD em seu projeto inicial era a Diretiva 95/46/CE que posteriormente fora substituída pelo GDPR. Ocorre que o projeto da lei brasileira só passou a ter maiores avanços nos trâmites legislativos após a aprovação do GDPR, de maneira a demonstrar a influência do efeito dominó acima explicitado. Pela análise dos relatórios do projeto de lei, também é possível verificar que, embora a lei tenha alto caráter protetivo em relação a direitos fundamentais como a privacidade, também fora proposta como um meio de garantir segurança das relações comerciais.

Como a Lei Geral de Proteção de Dados fora um marco legislativo temático, coube a ela agir doutrinariamente, de modo a também explicitar alguns conceitos. Dentre eles, podem-se destacar os seguintes verbetes: titular, para fazer alusão à pessoa natural a quem os dados se referem; tratamento: utilizado para referir-se a toda e qualquer operação envolvendo as informações pessoais do titular; dado pessoa: informação através da qual o titular (que deve ser pessoa física) é identificado ou identificável; dado pessoal sensível: relacionado: informação relacionada às escolhas e personalidade do indivíduo, como opinião política, orientação sexual, cor da pele, entre outros.

A LGPD também elencou princípios, que deverão sempre ser observados e respeitados, para guiar sua implementação e interpretação. Pode-se citar a trindade formada pelos princípios da finalidade (o tratamento de dados deve ser realizado para um fim anteriormente determinado e informado ao titular), necessidade (o tratamento será feito sob o menor tempo e envolvendo a mínima quantidade de dados possíveis), adequação (deve haver compatibilidade entre o tratamento realizado e sua finalidade). Salienta-se também o princípio do livre acesso, que garante ao titular dos dados meios para que tenha ciência de todos os detalhes envolvendo o tratamento de dados, bem como de solicitar retificação ou exclusão de suas informações pessoais.

Recorda-se ainda que a LGPD enumerou as chamadas bases legais de tratamento de dados. Estas também são conhecidas como opções autorizativas de tratamento, ou situações autorizantes e podem ser caracterizadas como as hipóteses taxativas e legalmente previstas que possibilitam o tratamento de dados. Cita-se algumas delas: consentimento expresso do titular, para o exercício regular de direitos em processos judiciais, para o cumprimento de obrigação

legal. Observa-se, por fim, que as bases de tratamento dos dados sensíveis são elencadas no artigo 11 da LGPD e dos dados pessoais no artigo 7º.

Ante todo o exposto, convém investigar a confluência entre o a Lei Geral de Proteção de Dados e o ambiente laboral. Inicialmente, pode-se assevera que é possível a aplicação da LGPD sobre o ambiente laboral, uma vez que: verifica-se que as transações envolvendo dados pessoais são parte do cotidiano no ambiente laboral; que também a personalidade é requisito da relação de emprego, de maneira que sempre haverá a presença de um empregado pessoa física que terá seus dados tratados; ainda pelo fato de que a LGPD não exclui expressamente, através de seu artigo 4º, as relações de trabalho e o Direito Laboral de sua aplicabilidade; também pela interpretação supletiva da LGPD através do direito comparado do GDPR (prevê aplicação no âmbito laboral), através do artigo 8º da Consolidação das Leis do Trabalho; e devido à harmonização entre dos princípios do Direito do Trabalho, da proteção de dados e da Lei Geral de Proteção de Dados.

No tocante às bases legais de tratamento, fora feito exame específico sobre o uso do consentimento, de modo a concluir que seu uso no tratamento de dados nas relações trabalhistas deve ser evitado e feito como última alternativa. Isso ocorre, pois a subordinação inerente à relação de emprego interfere na adjetivação “livre” do consentimento, restando dúvidas a respeito de sua legitimação. Aliado a isso, emerge o princípio da proteção ao trabalhador em sua acepção *in dubio pro operario* de maneira a deslegitimar o consentimento como base autorizativa de tratamento de dados dos trabalhadores.

No que se refere ao tratamento de dados em processos seletivos e análises curriculares, algumas considerações podem ser pontuadas. A princípio, entende-se que o consentimento, cumulado com o procedimento preliminar para execução de contrato são as bases legais escolhidas para tanto. Além disso, alguns cuidados devem ser tomados, como por exemplo: informar o titular previamente a respeito da finalidade da recolha de seus dados, bem colheita de seu consentimento e de cópias de documentos que autentiquem sua identidade. Para isso, aconselha-se o uso de formulários para os currículos digitais, sendo interessante também a guarda de seu *Internet Protocol* (IP).

Já no caso dos dados currículos envolvendo estagiários, aprendizes e outros processos seletivos com presença de adolescentes, algumas precauções extras dever ser tomadas. Defende-se que deve ser feita a colheita do consentimento dos pais e responsáveis do candidato menor de dezoito anos, além de angariar documentos que provem não apenas a identidade do responsável, como também sua relação com o candidato.

Inserido no ambiente laboral, têm-se os Direitos Coletivos do trabalhador, com destaque para as negociações coletivas. Isso ocorre pela interpretação supletiva da LGPD através de análise do GDPR. Todavia, alguns cuidados devem ser observados: há indicação de que a norma coletiva preveja mecanismos para facilitar a instituição da LGPD e seus procedimentos na seara laboral, além de também haver necessidade de observância dos requisitos convencionais para aprovação de Acordos e Convenções Coletivas do Trabalho. Assim, serão garantidos maior transparência e segurança jurídica para o tratamento de dados.

Entretanto o negociado não prevalecerá sobre o legislado quando o assunto estiver relacionado com a proteção de dados. Isso ocorre, pois a interpretação supletiva do direito comparado não permite também, por inconstitucionalidade do artigo 611-A da Consolidação das Leis do Trabalho e também por perigo de ofensas a direitos fundamentais constitucionais.

Ademais, convém salientar que as organizações de tendência tiveram sua gênese no direito alemão, de modo que podem ser caracterizadas através defesa ideológica de determinadas convicções pela empresa, ao ponto de ser a razão de sua existência, e possuem ainda como elementos caracterizadores o pluralismo, a livre iniciativa, e constituem-se também como forma de garantir direitos fundamentais de seus integrantes.

Como a ideologia possui grande relevância para as organizações de tendência e ainda é relacionada a dados sensíveis, o tratamento deste gênero de informações pessoais fará parte do cotidiano dessas empresas. Para isso, a empresa deverá fazer o uso da base legal de tratamento que garanta o exercício regular de direitos (já que o direito à livre iniciativa e a defesa de pensamento são direitos constitucionais do empregador) e garantir ainda o mínimo possível de dados sensíveis afetados. Logo, o tratamento de dados sensíveis será feito apenas para os trabalhadores portadores de tendência, vez que são os únicos imprescindíveis para a finalidade de organização ao contrário dos dados relativos aos trabalhadores neutros.

A Administração Pública, por outro lado, possui alguns deveres e princípios constitucionais que devem respeitar, como no caso do princípio da publicidade. Este obriga que aquela mantenha portais de transparência de modo a divulgar seus gastos à população. Dentre estes, destaca-se a divulgação da remuneração relacionada aos nomes completos dos empregados públicos, que são servidores público celetistas, ou seja, possuem contrato de trabalho regulado pelas normas trabalhistas, de modo que a Justiça do Trabalho possui competência sobre as causas que os envolvem.

Como a remuneração atrelada aos nomes podem significar parte da privacidade dos empregados públicos, restam dúvidas acerca de como a LGPD pode influenciar essa relação. Embora se entenda que a divulgação da remuneração é válida, o princípio da necessidade

contido na LGPD impõe que outros dados pessoais não precisam ser divulgados, como no caso do nome do empregado público. Para isso, entende-se como fundamental a adoção da técnica de pseudonimização de dados (substituindo o nome por um pseudônimo), que garante a privacidade ao indivíduo e não impede a fiscalização dos gastos públicos. Assim, é possível uma maior harmonização entre os princípios da publicidade e necessidade.

Por fim, cita-se o término de tratamento de dados. Primeiramente, enfoca-se no fim das operações sobre processos seletivos e currículos. Em regra, atingida a finalidade do tratamento de dados, estes deverão ser excluídos das bases de dados. Neste caso, devem ser observadas as prescrições trabalhistas de dois ou cinco anos.

Se o candidato desejar a manutenção de seu currículo na base de dados, deve fazer pedido reiterando, de modo que seria interessante que a empresa o armazenasse por mais seis meses (cabendo adiamento caso seja novamente reiterado) ou até o início de novo processo seletivo. Além disso, é possível a guarda dos dados pessoais dos candidatos para fins estatísticos internos da empresa, de maneira que seria aconselhável o uso da técnica da anonimização de dados, já que desvincula totalmente os dados de seu titular.

No caso do término do contrato de trabalho, alguns detalhes devem ser examinados. A análise deve ser feita de modo casuístico, já que não é possível uma delimitação temporal padrão do armazenamento dos dados do ex-empregado e sim uma delimitação circunstancial. Devem ser utilizadas as bases legais de tratamento relativas à obrigação legal e ao exercício de direito em processo. Caso o processo judicial, administrativo ou arbitral não seja iniciado, deve-se observar o prazo da prescrição bienal. Por outro lado, caso seja pleiteada ação judicial relativa ex-empregado, ou caso haja alguma possibilidade de surgimento de doença ocupacional futuramente manifestável, os dados poderão ser armazenados por tempo indeterminado.

REFERÊNCIAS

AGÊNCIA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA; CONSELHO DA EUROPA - TRIBUNAL EUROPEU DOS DIREITOS DO HOMEM. **Handbook on European data protection law**. Luxemburgo: Publications Office of the European Union, 2018. Disponível em: <https://op.europa.eu/en/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1>. Acesso em: 12 set. 2021.

ALMEIDA, Victor Hugo de; FERREIRA FILHO, Aluisio Ribeiro. Reflexos da lei de proteção de dados na fase pré-contratual trabalhista: desafios e medidas de proteção aos dados curriculares. *In: Seminário Internacional do Núcleo de Pesquisa e Observatório Jurídico “(Re)Pensando o Trabalho Contemporâneo” (RETRAB)*. 2020. Franca. **Anais [...]** Franca: UNESP, 2020, p. 829-840. Disponível em: https://www.franca.unesp.br/Home/Departamentos31/direitoprivado/anaisdeeventos/26.04.-02-anais_repensandoretrab_2020_final.pdf. Acesso em: 08 out. 2021.

AMORIM, Juliana Campelo de. A ressignificação do poder diretivo do empregador no contexto das organizações de tendência. **Revista do Direito UNIFACS - Debate Virtual**, Salvador, n. 237, 2020. Disponível em: <https://revistas.unifacs.br/index.php/redu/article/viewFile/6398/3897>. Acesso em: 22 out. 2021.

ARAÚJO, Douglas da Silva. Covid-19 e a “transparência” de dados pessoais dos beneficiários do auxílio emergencial à luz da lei geral de proteção de dados. **Boletim de Conjuntura (BOCA)**, Boa Vista, v. 3, n. 8, p. 17-21, jul. 2020. Disponível em: <https://revista.ufrb.br/boca/article/view/Araujo/3038>. Acesso em: 16 out. 2021.

ASSUNÇÃO, Carolina Silva Sílvinio; KOURY, Luiz Ronan Neves. Lei Geral de Proteção de Dados - LGPD: aspectos principais- repercussão no direito material e direito processual do trabalho. *In: AMADO, Renato de Paula; LIMA, Leonardo Tibo Barbosa. (Orgs). Lei geral de proteção de dados pessoais: impactos na seara trabalhista*. Edição do Kindle. Belo Horizonte: AMATRA 3: RTM, 2021. p. 121-142.

AZEVEDO, Laura Machado de Souza; MACHADO, Daniela Cunha. Direitos à privacidade, à intimidade e à autodeterminação informativa. *In: MIZIARA, Raphael; PESSOA, André; MOLLICIONE, Bianca (orgs.). Reflexos da LGPD no Direito e no Processo do Trabalho*. São Paulo: Thomson Reuters Brasil, 2020. p. 173-184.

BENACCHIO, Marcelo; MACIEL, Renata Mota. A LGPD sob a Perspectiva da Regulação do Poder Econômico. *In: LIMA, Cíntia Rosa Pereira de. (Org.). Comentários à Lei Geral de Proteção de Dados*. São Paulo: Grupo Almedina, 2020. p. 39-68. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788584935796/pageid/39>. Acesso em: 07 set. 2021.

BEZERRA, Mirthyani. Lei Geral de Proteção de Dados entra em vigor nesta sexta; veja o que muda... **TILT UOL**, São Paulo, 18 set. 2020. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2020/09/18/bolsonaro-sanciona-vigencia-imediata-da-lei-de-protecao-de-dados.htm>. Acesso em: 18 set. 2021.

BINENBOJM, Gustavo. O princípio da publicidade administrativa e a eficácia da divulgação de atos do poder público pela internet. **REDE - Revista Eletrônica de Direito do Estado**, Salvador, n. 19, jul./ago. 2009. Disponível em: <http://www.direitodoestado.com.br/codrevista.asp?cod=348>. Acesso em: 10 out. 2021.

BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado. **Cadernos Jurídicos**, São Paulo, ano 21, n° 53, p. 191-201, jan./mar. 2020,. Disponível em: https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_9_anonimizacao_e_dado.pdf?d=637250349860810398. Acesso em: 06 de out. 2021.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais - A função e os limites do consentimento**. Rio de Janeiro: Grupo GEN, 2021. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788530994105/>. Acesso em: 07 set. 2021.

BOMFIM, Vólia; PINHEIRO, Iuri. A Lei Geral de Proteção de Dados e seus impactos nas relações de trabalho. *In*: MIZIARA, Raphael; PESSOA, André; MOLLICIONE, Bianca. **Reflexos da LGPD no Direito e no Processo do Trabalho**. São Paulo: Thomson Reuters Brasil, 2020. p. 148-73.

BRASIL. Projeto de Lei n° 4060/2012. Dispõe sobre a proteção de dados pessoais e altera a Lei n° 12.965, de 23 de abril de 2014. **Câmara dos Deputados**, Brasília, DF, 2012. Disponível em: www.camara.leg.br/propostas-legislativas/548066. Acesso em: 19 set. 2021.

BRASIL. Constituição da República Federativa do Brasil de 1988. **Diário Oficial da União**, Brasília, DF, 5 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 08 set. 2021.

BRASIL. Decreto-lei n° 5.452, de 1° de maio de 1943. Aprova a Consolidação das Leis do Trabalho. **Diário Oficial da União**, Rio de Janeiro, 1 maio 1943. Disponível em: www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm. Acesso em: 19 out. 2021.

BRASIL. Lei n 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. **Diário Oficial da União**, Brasília, DF, 13 jul. 1990b. Disponível em: www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 08 out. 2021.

BRASIL. Lei n° 10.097, de 19 de dezembro de 2000. Altera dispositivos da Consolidação das Leis do Trabalho – CLT, aprovada pelo Decreto-Lei no 5.452, de 1° de maio de 1943. **Diário Oficial da União**, Brasília, DF, 19 dez. 2000. Disponível em: www.planalto.gov.br/ccivil_03/LEIS/L10097.htm. Acesso em: 09 out. 2021.

BRASIL. Lei n° 11.788, de 25 de setembro de 2008. Dispõe sobre o estágio de estudantes; altera a redação do art. 428 da Consolidação das Leis do Trabalho – CLT, aprovada pelo Decreto-Lei no 5.452, de 1o de maio de 1943, e a Lei no 9.394, de 20 de dezembro de 1996; revoga as Leis nos 6.494, de 7 de dezembro de 1977, e 8.859, de 23 de março de 1994, o parágrafo único do art. 82 da Lei no 9.394, de 20 de dezembro de 1996, e o art. 6o da Medida Provisória no 2.164-41, de 24 de agosto de 2001; e dá outras providências. **Diário Oficial da União**, Brasília, DF, 25 set. 2008. Disponível em: www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11788.htm. Acesso em: 09 out. 2021.

BRASIL. Lei nº 12.527, de 18 de novembro de 2021. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. **Diário Oficial da União**, DF, 18 nov. 2011. Disponível em: www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112527.htm. Acesso em: 10 out. 2021.

BRASIL. Lei nº 13.105, de 16 de março de 2015. Código de Processo Civil. **Diário Oficial da União**, Brasília, DF, 13 mar. 2015b. Disponível em: www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/113105.htm. Acesso em 18 out. 2021.

BRASIL. Lei nº 9.784, de 29 de janeiro de 1999. Regula o processo administrativo no âmbito da Administração Pública Federal. **Diário Oficial da União**, Brasília, DF, 29 jan. 1999. Disponível em: www.planalto.gov.br/ccivil_03/leis/19784.htm. Acesso em: 10 out. 2021.

BRASIL. Lei nº 11.180, de 23 de setembro de 2005. Institui o Projeto Escola de Fábrica, autoriza a concessão de bolsas de permanência a estudantes beneficiários do Programa Universidade para Todos – PROUNI, institui o Programa de Educação Tutorial – PET, altera a Lei nº 5.537, de 21 de novembro de 1968, e a Consolidação das Leis do Trabalho – CLT, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943, e dá outras providências. **Diário Oficial da União**, Brasília, DF, 23 set. 2005. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Lei/L11180.htm. Acesso em: 09 out. 2021.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**, Brasília, DF, 23 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 14 set. 2021.

BRASIL. Lei nº 13.467, de 13 de julho de 2017. Altera a Consolidação das Leis do Trabalho (CLT), aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943, e as Leis nº 6.019, de 3 de janeiro de 1974, 8.036, de 11 de maio de 1990, e 8.212, de 24 de julho de 1991, a fim de adequar a legislação às novas relações de trabalho. **Diário Oficial da União**, Brasília, DF, 13 jul. 2017a. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Lei/L13467.htm. Acesso em: 18 out. 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Brasília, DF, 14 ago. 2018a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 15 set. 2021.

BRASIL. Lei nº 13.853, de 08 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. **Diário Oficial da União**, Brasília, DF, 08 jul. 2019a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/113853.htm. Acesso em: 02 out. 2021.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. **Diário Oficial da União**, Brasília, DF, 11 set. 1990a. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/18078compilado.htm. Acesso em: 12 set. 2021.

BRASIL. Mensagem nº 451, de 14 de agosto de 2018. **Diário Oficial da União**, Brasília, 2018b. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-veto-156214-pl.html>. Acesso em: 19 de set. 2021.

BRASIL. Ministério Público do Trabalho. Nota Técnica nº 08, de 26 de junho de 2017, da Secretaria de Relações Institucionais do Ministério Público do Trabalho (MPT), subscrita pelo Dr. Ronaldo Curado Fleury, Procurador Geral do Trabalho. Brasília, DF, 26 jun. 2017c. Disponível em: http://www.mpt.mp.br/pgt/publicacoes/notas-tecnicas/nota-tecnica-ndeg8/@@download/arquivo_pdf. Acesso em: 21 out. 2021.

BRASIL. Superior Tribunal de Justiça. Acórdão de decisão que negou, por unanimidade, conhecimento ao recurso. Recurso Especial nº 22.337/RS. Relator: Ministro Ruy Rosado de Aguiar. Brasília, DF, 13 fev. 1995. Disponível em: https://processo.stj.jus.br/processo/ita/documento/mediado/?num_registro=199200114466&dt_publicacao=20-03-1995&cod_tipo_documento=&formato=PDF. Acesso em: 26 set. 2021.

BRASIL. Superior Tribunal de Justiça. Acórdão de decisão que, por unanimidade, deu parcial provimento ao recurso especial. Recurso Especial nº 1.348.53/SP. Relator: Ministro Luis Felipe Salomão. Brasília, DF, 30 nov. 2017b. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencia=1646430&num_registro=201202108054&data=20171130&peticao_numero=-1&formato=PDF. Acesso em: 26 set. 2021.

BRASIL. Supremo Tribunal Federal. Acórdão, apreciando o tema 483 de repercussão geral, deu provimento ao recurso extraordinário, fixando-se a tese de que é legítima a publicação, inclusive em sítio eletrônico mantido pela Administração Pública, dos nomes dos seus servidores e do valor dos correspondentes vencimentos e vantagens pecuniárias, nos termos do voto do Relator.. Recurso Especial com Agravo nº 652.777/SP. Relator: Ministro Teoria Zavascki. Brasília, DF, 23 abr. 2015. Disponível em: <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=8831570>. Acesso em: 10 out. 2021.

BRASIL. Supremo Tribunal Federal. Despacho. Recurso Extraordinário com Agravo 1.121.633-Goiás. Relator: Ministro Gilmar Mendes. Brasília, DF, 28 jun. 2019b. Disponível em: redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=750241640&prcID=5415427&ad=s#. Acesso em: 21 out. 2021.

BRUE, Stanley L. **História do pensamento econômico**. São Paulo: Pioneira Thomson Learning, 2005.

BYGRAVE, Lee A.; TOSONI, Luca. Article 4(11). Consent. In: KUNER, Christopher; BYGRAVE, Lee A.; DUCKSEY, Christopher. (Coords). **The UE General Data Protection Regulation: a commentary**. Oxford: Oxford University Press, 2020. p. 174-187.

CACHAPUZ, Maria Cláudia Mércio. Privacidade, proteção de dados e autodeterminação informativa. **Revista Jurídica da Presidência**, Brasília, v. 15, n. 107, p. 823-848, 2014. Disponível em: <https://doi.org/10.20499/2236-3645.RJP2014v15e107-126>. Acesso em: 11 set. 2021.

CARLOTO, Selma. **A Lei geral de Proteção de Dados: com enfoque nas relações de trabalho**. 2. ed. São Paulo: LTr, 2021.

CARLOTO, Selma; GUERRA, Elaine. **Manual Prático de Adequação à LGPD: com enfoque nas relações de trabalho**. Edição do Kindle. São Paulo: LTr, 2021.

CARVALHO FILHO, José dos Santos. **Manual de Direito Administrativo**. São Paulo: Atlas, 2020. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788597024982/>. Acesso em: 10 out. 2021

CASSAR, Vólia Bomfim. **Direito do Trabalho: de acordo com a reforma trabalhista**. 16. ed. rev. e atual. Rio de Janeiro: Forense; São Paulo: Método, 2018.

CAVALCANTE, Sóstenes. Comissão de Ciência e Tecnologia, Comunicação e Informática (CCTCI). Apresentação do Parecer do Relator n. 1 CCTCI, pelo Deputado Sóstenes Cavalcante (DEM-RJ). **Câmara dos Deputados**, Brasília, DF, 2016. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=8B1B0A4EB9A45DFBB9CCE28ABCCC0EE7.proposicoesWebExterno2?codteor=1454623&filename=Tramitacao-PL+4060/2012. Acesso em: 19 set. 2021.

CAVOUKIAN, Ann. Privacy by Design. The 7 Foundational Principles. **Information & Privacy Commissioner**, Ontario, mar. 2011. Disponível em: https://iab.org/wp-content/uploads/2011/03/fred_carter.pdf. Acesso em: 01 out. 2021.

CONI JÚNIOR, Vicente Vasconcelos; PAMPLONA FILHO, Rodolfo. A Lei Geral de Proteção de Dados Pessoais e seus impactos no Direito do Trabalho. **Revista do Direito UNIFACS - Debate Virtual**, Salvador. n. 249, 2021. Disponível em: <https://revistas.unifacs.br/index.php/redu/article/view/6744/4066>. Acesso em: 02 out. 2021.

CONI JÚNIOR, Vicente Vasconcelos; PAMPLONA FILHO, Rodolfo. A Lei Geral de Proteção de Dados e seus reflexos nas relações jurídicas trabalhistas. *In*: MIZIARA, Raphael; PESSOA, André; MOLLICIONE, Bianca. (Orgs.). **Reflexos da LGPD no Direito e no Processo do Trabalho**. São Paulo: Thomson Reuters Brasil, 2020. p. 74-124.

CUEVA, Ricardo Villas Bôas. A insuficiente proteção de dados pessoais no Brasil. **Revista Justiça e Cidadania**, Rio de Janeiro, ed. 195, p. 8-3, novembro de 2016. Disponível em: https://editorajc.com.br/wp-content/uploads/2016/12/RJC-195_.pdf. Acesso em: 12 set. 2021.

D'ALMEIDA, Érica Nogueira Soares. **Disseminação não consensual de imagens íntimas: uma análise à luz do Regulamento Geral de Proteção de Dados**. Orientadora: Ana Mafalda Castanheira Neves de Miranda Barbosa. 2020. 170f. Dissertação (Mestrado em Ciências Jurídico-Políticas/Menção em Direito Internacional Público e Europeu) – Universidade de Coimbra, Faculdade de Direito da Universidade de Coimbra, Coimbra, 2020. Disponível em: <https://eg.uc.pt/handle/10316/92692>. Acesso em: 12 set. 2021.

DE HERT, Paul; LAMMERANT, Hans. **Protection of personal data in work-related relations**. Study made on behalf of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs. Brussels: European Parliament, 2013. Disponível em: [https://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/474440/IPOL-LIBE_ET\(2013\)474440_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/474440/IPOL-LIBE_ET(2013)474440_EN.pdf). Acesso em: 20 out. 2021.

DELGADO, Mauricio Godinho. **Curso de direito do trabalho**: obra revista e atualizada conforme a lei da reforma trabalhista e inovações normativas e jurisprudenciais posteriores - 18. ed. São Paulo: LTr, 2019.

DELGADO, Mauricio Godinho; DELGADO, Gabriela Neves. **A reforma trabalhista no Brasil**: com os comentários à Lei n. 13.467/2017. São Paulo: LTr, 2017.

DI PIETRO, Maria Sylvia Zanella. **Direito Administrativo**. Rio de Janeiro: Forense, 2021. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788530993351/>. Acesso em: 10 out. 2021.

DÖHMANN, Indra Spiecker Gen. A proteção de dados pessoais sob o Regulamento Geral de Proteção de Dados da União Europeia. *In*: BIONI, Bruno; DONEDA, Danilo; MENDES, Laura Schertel; RODRIGUES JÚNIOR, Otavio Luiz; SARLET, Ingo Wolfgang. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: GEN, 2020. p. 113-129. Disponível em: [https://integrada.minhabiblioteca.com.br/reader/books/9788530992200/epubcfi/6/30\[%3Bvnd.vst.idref%3Dhtml14\]!/4](https://integrada.minhabiblioteca.com.br/reader/books/9788530992200/epubcfi/6/30[%3Bvnd.vst.idref%3Dhtml14]!/4). Acesso em: 12 set. 2021.

DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2020b.

DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. *In*: BIONI, Bruno; DONEDA, Danilo; MENDES, Laura Schertel; RODRIGUES JÚNIOR, Otavio Luiz; SARLET, Ingo Wolfgang. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: GEN, 2020a, p. 22-39. Disponível em: [https://integrada.minhabiblioteca.com.br/reader/books/9788530992200/epubcfi/6/22\[%3Bvnd.vst.idref%3Dhtml10\]!/4/2/4/1:0\[%2C1\]](https://integrada.minhabiblioteca.com.br/reader/books/9788530992200/epubcfi/6/22[%3Bvnd.vst.idref%3Dhtml10]!/4/2/4/1:0[%2C1]). Acesso em: 12 set. 2021.

DONEDA, Danilo. Proteção de Dados Pessoais. *In*: GALDINO, Flávio; KATAOKA, Eduardo Takemi; TORRES, Ricardo Lobo. (Orgs.).v **Dicionário de princípios jurídicos**. Rio de Janeiro: Elsevier, 2011. p. 1.141-1.148.

EECKE, Patrick Van; ŠIMKUS, Anrijs. Article 88.Processing in the context of employment. *In*: KUNER, Christopher; BYGRAVE, Lee A.; DUCKSEY, Christopher. (Coords). **The UE General Data Protection Regulation**: a commentary. Oxford: Oxford University Press, 2020. p. 1129-1139.

EUROPEAN COMISSION. **General Data Protection Regulation (GDPR)** – Official Legal Text. Recital 43: Freely Given Consent. Luxembourg: Publications Office of the European Union, 2018. Disponível em: <https://gdpr-info.eu/recitals/no-43/>. Acesso em: 03 out. 2021.

FERREIRA FILHO, Manoel Gonçalves. **Curso de Direito Constitucional**. Rio de Janeiro: GEN, 2020. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788530991845/>. Acesso em 4 set. 2021.

FLUMIGNAN, Silvano J. G.; FLUMIGNAN, Wévertton G. G. Princípios que Regem o Tratamento de Dados no Brasil. In: LIMA, Cíntia Rosa P. (Coord). **Comentários à lei geral de proteção de dados: Lei n. 13.709/2018, com alteração da lei n.13.853/2019**. São Paulo: Almedina, 2020. p. 123-140. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788584935796/pageid/123>. Acesso em: 26 set. 2021.

FONSECA, Maria Hemília. **Curso de metodologia na elaboração de trabalhos acadêmicos**. Rio de Janeiro: Ciência Moderna, 2009.

FONSECA, Maurício Leopoldino da; NOGUEIRA, Fernanda Araújo e Melo. O consentimento na Lei Geral de Proteção de Dados: autonomia privada e o consentimento livre, informado e expresse. In: GROSSI, Bernardo Menicucci. **Lei Geral de Proteção de Dados: uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial**. Porto Alegre: Fi, 2020. p. 15-44. Disponível em: <https://www.editorafi.org/21dados>. Acesso em: 17 out. 2021.

FRAZÃO, Ana. Nova LGPD: a importância do consentimento para o tratamento dos dados pessoais. **JOTA**, São Paulo, 12 set. 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-a-importancia-do-consentimento-para-o-tratamento-dos-dados-pessoais-12092018>. Acesso em: 03 out. 2021.

FREITAS, Bruna S. Jardim. A LGPD e os impactos sobre o tratamento de dados pessoais de adolescentes nas relações de trabalho. **Revista Direito UNIFACS–Debate Virtual**, Salvador, n. 246, dez. 2020. Disponível em: <https://revistas.unifacs.br/index.php/redu/article/view/6962>. Acesso em: 09 out. 2021.

GASPAR, Gabriela Curi Ramos. **Colisão de direitos fundamentais nas relações de emprego em organizações de tendência**. Orientador: Rodolfo Mário Veiga Pamplona Filho. Dissertação (Mestrado) - Universidade Federal da Bahia, Faculdade de Direito, Salvador, 2015. Disponível em: <http://repositorio.ufba.br/ri/handle/ri/17260>. Acesso em: 22 out. 2021.

GASPAR, Gabriela Curi Ramos. LGPD e o tratamento de dados sensíveis nas organizações de tendência. In: MIZIARA, Raphael; PESSOA, André; MOLLICIONE, Bianca. (Orgs.). **Reflexos da LGPD no Direito e no Processo do Trabalho**. São Paulo: Thomson Reuters Brasil, 2020. p. 200-231.

GOMES, Helton Simões; PADRÃO, Márcio. Proteção de dados pessoais se torna lei no Brasil com veto a “xerife”. **TILT UOL**, São Paulo, 14 ago. 2018. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2018/08/14/temer-sanciona-lei-brasileira-de-protecao-de-dados-pessoais-tire-duvidas.htm>. Acesso em: 19 set. 2021.

GONÇALVES, Marcus Vinicius Rios. **Direito processual civil - Esquematizado**. São Paulo: Saraiva, 2020. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788553615933/>. Acesso em: 18 out. 2021.

GUIMARÃES FILHO, Pedro Andrade; FERNEDA, Ariê Scherreier; FERRAZ, Miriam Olivia Knopik. A proteção de dados e a defesa do consumidor: autonomia privada frente à privacidade. **Revista Meritum**, Belo Horizonte, v. 15, n. 2, p. 38-52, maio/ago. 2020. Disponível em: <http://revista.fumec.br/index.php/meritum/article/view/7749>. Acesso em: 14 set. 2021.

HAN, Byung-Chul. **Sociedade da Transparência**. Tradução Enio Paulo Giachini. Petrópolis: Vozes, 2017.

HILL, Kashmir. How Target figured out a teen girl was pregnant before her father did. **Forbes**, Nova Iorque, 12 fev. 2012. Disponível em: <https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=4901222a6668>. Acesso em: 08 set. 2021.

INTERNATIONAL LABOR ORGANIZATION. **Application of international labour standards 2017 (I)**: Report of the committee of experts on the application of conventions and recommendations. Geneva: International labour office, 2017. Disponível em: [https://www.ilo.org/public/libdoc/ilo/P/09661/09661\(2017-106-1A\).pdf](https://www.ilo.org/public/libdoc/ilo/P/09661/09661(2017-106-1A).pdf). Acesso em: 20 out. 2021.

INTERNATIONAL LABOR ORGANIZATION. **Protection of workers' personal data**. An ILO code of practice. Geneva: International Labour Office, 1997. Disponível em: www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf. Acesso em: 19 out. 2021.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de Metodologia Científica**. 5. ed. São Paulo: Atlas, 2003.

LARA, Rodrigo; TAGIAROLI, Guilherme. Por que as propagandas nos 'perseguem' na web? É perigoso? Como se livrar? **Tilt UOL**, São Paulo, 27 jul. 2021. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2021/07/27/propagandas-perseguem-voce-na-web-saiba-como-esses-anuncios-funcionam.htm>. Acesso em: 08 set. 2021.

LEITE, Carlos Henrique Bezerra. **Curso de direito do trabalho**. 13. ed. São Paulo: Saraiva Educação, 2021a. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555595680/>. Acesso em 02 out. 2021.

LEITE, Carlos Henrique. Bezerra. **Curso de Direito Processual do Trabalho**. São Paulo: Editora Saraiva, 2021b. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555593983/>. Acesso em: 18 out. 2021.

LIMA, Ana Luíza Argolo Cavalcante. **A (in)constitucionalidade da flexibilização dos direitos e garantias trabalhistas contida no artigo 611-a da lei da reforma trabalhista (lei 13.467/2017) sob o prisma do princípio da proibição do retrocesso social**. Orientador: Gabriel Dias Marques da Cruz. 79 f. 2017. Monografia (Trabalho de Conclusão do Curso de Graduação em Direito) – Universidade Federal da Bahia, Salvador, 2017. Disponível em: <http://repositorio.ufba.br/ri/handle/ri/24842>. Acesso em: 21 out. 2021.

LIMA, Caio César Carvalho. Capítulo II - Do tratamento de dados. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD: Lei Geral de Proteção de Dados comentada**. – 2. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2020. p. 201-241.

LIMA, Gabriela Vasconcelos; DIAS, Eduardo Rocha. Sopesamento entre o princípio da publicidade e o direito à privacidade na sociedade informacional: uma crítica hermenêutica à aplicação da lei de colisão de Alexy no Brasil. **Revista de Direito Brasileira**, [S.l.], v. 16, n. 7, p. 5-20, abr. 2017. Disponível em: <https://www.indexlaw.org/index.php/rdb/article/view/2968/2751>. Acesso em: 16 out. 2021.

MACHADO, Joana de Moraes Souza. A expansão do conceito de privacidade e a evolução na tecnologia de informação com o surgimento dos bancos de dados. **Revista AJURIS - Associação dos Juizes do Rio Grande do Sul**, Porto Alegre, v. 42, n. 134, p. 337-363, 2014. Disponível em: <http://ajuris.kinghost.net/OJS2/index.php/REVAJURIS/article/view/206>. Acesso em: 11 set. 2021.

MANSOUR, Isla Maria Amorim de Souza. **O STF e a divulgação nominalmente individualizada da remuneração dos servidores públicos**: uma análise crítica do recurso extraordinário 652.777-SP. Orientador: Argemiro Cardoso Moreira Martins. 2017. 133 f. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de Brasília, Brasília, 2017. Disponível em: <https://repositorio.unb.br/handle/10482/31106>. Acesso em: 16 out. 2021.

MARCACINI, Augusto Tavares Rosa. Regras Aplicadas ao Tratamento de Dados Pessoais. *In*: LIMA, Cíntia Rosa Pereira de (Org.). **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020. p. 141-162. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788584935796/pageid/141>. Acesso em: 07 set. 2021.

MARQUES, Maria da Conceição da Costa. Aplicação dos Princípios da Governança Corporativa Aplicação dos Princípios da Governança Corporativa ao Sector Público. **Revista de Administração Contemporânea**, João Pessoa, v. 11, n. 2, p. 11-26, 2011. Disponível em: <https://doi.org/10.1590/S1415-6552007000200002>. Acesso em: 02 out. 2021.

MARTIAL-BRAZ, Nathalia. O direito das pessoas interessadas no tratamento de dados pessoais: anotações da situação na França e na Europa. **Revista de Direito, Estado e Telecomunicações**, Brasília, v. 10, n. 1, p. 85-108, maio 2018. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/Rev-Dir-Est-Telecom_v.10_n.01.05.pdf. Acesso em: 12 set. 2021.

MARTINEZ, Luciano. **Curso de Direito do Trabalho**. 11. ed. São Paulo: Saraiva Educação, 2020. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788553618408/>. Acesso em: 03 out. 2021.

MARTINEZ, Luciano. **Reforma trabalhista – entenda o que mudou**: CLT comparada e comentada. 2. ed. São Paulo: Saraiva Educação, 2018. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788553600885/>. Acesso em: 19 out. 2021.

MARTINS, Marcelo Guerra; TATEOKI, Victor Augusto. Proteção de dados pessoais e democracia: fake news, manipulação do eleitor e o caso da Cambridge Analytica. **REDES - Revista Eletrônica Direito e Sociedade**, Canoas, v. 7, n. 3, p. 115-138, 2019. Disponível em: <https://revistas.unilasalle.edu.br/index.php/redes/article/view/5610>. Acesso em: 17 out. 2021.

MATOS, Larissa. Princípios da Lei Geral de Proteção de Dados. *In*: MIZIARA, Raphael; PESSOA, André; MOLLICIONE, Bianca. (Orgs.). **Reflexos da LGPD no Direito e no Processo do Trabalho**. São Paulo: Thomson Reuters Brasil, 2020. p. 15-28.

MAZZA, Alexandre. **Manual de Direito Administrativo**. São Paulo: Saraiva Educação, 2021. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555593266/>. Acesso em: 10 out. 2021.

MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. **Pensar – Revista de Ciências Jurídicas**, Fortaleza, v. 25, n. 4, p. 1-18, 2020. Disponível em: <https://periodicos.unifor.br/rpen/article/view/10828>. Acesso em: 11 set. 2021.

MENDES, Laura Schertel. Habeas data e autodeterminação informativa. **Revista Brasileira de Direitos Fundamentais & Justiça**, Belo Horizonte, v. 12, n. 39, p. 185-216, 26 mar. 2019. Disponível em: <http://dfj.emnuvens.com.br/dfj/article/view/655/905>. Acesso em: 13 set. 2021.

MIYAGUSUKU, Jorge Toyama. **Derechos inespecíficos de los trabajadores en los empleadores ideológicos**. Orientador: Francisco Eguiguren Praeli. 2008. 314 f. Dissertação (Mestrado) - Pontificia Universidad Católica del Perú, Escuela de Graduados, San Miguel, 2008. Disponível em: <http://hdl.handle.net/20.500.12404/4686>. Acesso em: 22 out. 2021.

MONTI, Milton. Projeto de Lei nº __, de 2012. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. **Câmara dos Deputados**, Brasília, DF, 2012. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1001750. Acesso em: 19 set. 2021.

MORAES, Alexandre de. **Direito Constitucional**. São Paulo: GEN, 2021. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788597027648/>. Acesso em: 08 set. 2021.

MOREIRA, José Carlos Barbosa. O habeas data brasileiro e sua lei regulamentadora. **Revista de Direito Administrativo**, Revista da EMERJ, Rio de Janeiro, v. 1, n. 1, 1998. Disponível em: https://www.emerj.tjrj.jus.br/revistaemerj_online/edicoes/revista01/revista01_16.pdf. Acesso em: 13 set. 2021.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. Privacy Myths and Fallacies of “Personally Identifiable Information”. **Communications of the ACM**, Nova Iorque, n. 06, v. 53, p. 24-26, jun. 2010. Disponível em: <https://cacm.acm.org/magazines/2010/6/92489-myths-and-fallacies-of-personally-identifiable-information/fulltext>. Acesso em: 06 de out. 2021.

NASCIMENTO, André Pestana. O impacto das novas tecnologias no direito do trabalho e a tutela dos direitos de personalidade do trabalhador. **Uría Menéndez**, Lisboa, 2006. Disponível em: https://www.uria.com/documentos/publicaciones/2242/documento/068apa.pdf?id=1948_pt. Acesso em: 25 abr. 2021.

OLIVEIRA, Guilherme Henrique Gualtieri. As bases legais para o tratamento de dados pessoais: muito além do consentimento. *In*: GROSSI, Bernardo Menicucci. **Lei Geral de Proteção de Dados: uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial**. Porto Alegre: Fi, 2020. p. 45-63. Disponível em: <https://www.editorafi.org/21dados>. Acesso em: 21 ago. 2021.

OLIVEIRA, Letícia Costa. **O uso de dados pessoais na era digital como forma de manipulação social e ameaça a democracia: um estudo de caso da Cambridge Analytica**. Orientador: Danillo Alarcon. 2021. 63 f. Monografia (Trabalho de Conclusão do Curso de Graduação em Relações Internacionais) - Escola de Direito e Relações Internacionais - Pontifícia Universidade Católica de Goiás, Goiânia, 2021. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/handle/123456789/1870>. Acesso em: 17 out. 2021.

OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei n.13.709/2018. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 2. ed. São Paulo: RT Thomson Reuters Brasil, 2020. p. 53-83. Disponível em: <https://bdjur.stj.jus.br/jspui/handle/2011/138898>. Acesso em: 18 set. 2021.

OLIVEIRA, Rafael. Carvalho Rezende. **Princípios do Direito Administrativo**. 2. ed. Rio de Janeiro: Forense; São Paulo: Método, 2013. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/978-85-309-4939-6/>. Acesso em: 10 out. 2021.

PEREIRA, Alexandre Libório Dias. O Marco Civil da Internet e seus reflexos no Direito da União Europeia. **Revista Jurídica Luso-Brasileira**, Lisboa (Portugal), ano 2, n. 4, p. 53-106, 2016. Disponível em: www.cidp.pt/revistas/rjlb/2016/4/2016_04_0053_0106.pdf. Acesso em: 14 set. 2021.

PINCER, Pedro. Proteção de dados pessoais será incluída entre direitos fundamentais previstos na Constituição. **Senado Notícias**, Brasília, DF, 20 out. 2021. Disponível em: www12.senado.leg.br/noticias/audios/2021/10/protecao-de-dados-pessoais-sera-incluida-entre-direitos-fundamentais-previstos-na-constituicao. Acesso em: 21 out 2021.

PINHEIRO, Patrícia Peck. **Direito Digital**. 6. ed. São Paulo: Saraiva, 2016.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais: comentários à lei n. 13.709/2018 (LGPD)**. São Paulo: Saraiva, 2021. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555595123/>. Acesso em: 07 set. 2021.

PLÁ RODRIGUEZ, Américo. **Princípios do direito do trabalho**. 3. ed. São Paulo: LTr, 2000.

REIS, Raquel Tavares dos. Direitos, liberdades e garantias da pessoa do trabalhador despedido em razão da sua conduta extra-laboral. **Gestão e Desenvolvimento**, Viseu, n. 10, p. 95-127, 1 jan. 2001. Disponível em: <https://revistas.ucp.pt/index.php/gestaoedesenvolvimento/article/view/69>. Acesso em: 22 out. 2021.

RUARO, Regina Linden; SARLET, Gabrielle Bezerra Sales. O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da Lei Geral de Proteção de Dados (LGPD) - Lei 13.709/2018. *In*: BIONI, Bruno; DONEDA, Danilo; MENDES, Laura Schertel; RODRIGUES JÚNIOR, Otavio Luiz; SARLET, Ingo Wolfgang. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: GEN, 2020. p. 190-211. Disponível em: [https://integrada.minhabiblioteca.com.br/reader/books/9788530992200/epubcfi/6/40\[%3Bvnd.vst.idref%3Dhtml19\]!/4](https://integrada.minhabiblioteca.com.br/reader/books/9788530992200/epubcfi/6/40[%3Bvnd.vst.idref%3Dhtml19]!/4). Acesso em: 20 set. 2021.

RUIZ, Evandro Eduardo Seron. Anonimização, pseudonimização e desanonimização de dados pessoais. *In*: LIMA, Cíntia Rosa P. (Coord). **Comentários à lei geral de proteção de dados: Lei n. 13.709/2018, com alteração da lei n.13.853/2019**. São Paulo: Almedina, 2020. p 101-122. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788584935796/pageid/101>. Acesso em: 16 out. 2021.

SAES, Flávio Azevedo Marques de; SAES, Alexandre Macchione. **História Econômica Geral**. São Paulo: Saraiva, 2013. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788502212565/>. Acesso em: 07 set. 2021.

SAMPAIO, Alice Castaldi. **Data brokers: um novo modelo de negócios baseado em vigilância de dados** Orientadora: Marta Mourão Kanashiro. 2017. 135 f. Dissertação (Mestrado) – Universidade Estadual de Campinas, Instituto de Estudos da Linguagem, São Paulo 2007. Disponível em: <http://repositorio.unicamp.br/handle/REPOSIP/322483>. Acesso em: 08 set. 2021.

SANDEN, Ana Francisca Moreira de Souza. **A proteção de dados pessoais do empregado no direito brasileiro: um estudo sobre os limites na obtenção e no uso pelo empregador da informação relativa ao empregado**. São Paulo: LTr, 2014.

SILVA, Fabrício Lima. A autodeterminação informativa nas relações de trabalho: tensões e desafios. *In*: AMADO, Renato de Paula; LIMA, Leonardo Tibo Barbosa. (Orgs). **Lei geral de proteção de dados pessoais: impactos na seara trabalhista**. Edição do Kindle. Belo Horizonte: AMATRA 3: RTM, 2021, p. 41-60.

SILVA, Joana Luís da. **Big Data no comércio eletrônico: utilização de cookies e questões de privacidade na recolha de dados pessoais**. Orientadora: Ana Isabel Rojão Lourenço Azevedo. 2020. 95 f. Tese (Mestrado em Negócio Eletrónico) – Instituto Superior de Contabilidade e Administração do Porto Politécnico do Porto, São Mamede de Infesta (Portugal), 2020. Disponível em: <http://hdl.handle.net/10400.22/17368>. Acesso em: 07. Set. 2021.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 31. ed. São Paulo: Malheiros, 2008.

SILVA, ORLANDO. Comissão especial destinada a proferir parecer ao projeto de lei nº 4060, de 2012. Apresentação do Parecer do Relator, pelo Deputado Orlando Silva. **Câmara dos Deputados**, Brasília, DF, 2018. Disponível em:

https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filenome=PRL+1+PL406012+%3D>+PL+4060/2012. Acesso em: 19 set. 2021.

TEFFÉ, Chiara Spadaccini; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11. *In*: BIONI, Bruno; DONEDA, Danilo; MENDES, Laura Schertel; RODRIGUES JÚNIOR, Otavio Luiz; SARLET, Ingo Wolfgang. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: GEN, 2020a. p. 131-162. Disponível em: [https://integrada.minhabiblioteca.com.br/reader/books/9788530992200/epubcfi/6/34\[%3Bvnd.vst.idref%3Dhtml16\]!/4/2/4/1:0\[%2C6\]](https://integrada.minhabiblioteca.com.br/reader/books/9788530992200/epubcfi/6/34[%3Bvnd.vst.idref%3Dhtml16]!/4/2/4/1:0[%2C6]). Acesso em: 03 out. 2021.

TENA, Angel Luis de Val. Las empresas de tendencia ante el derecho del trabajo: libertad ideológica y contrato de trabajo. *Proyecto social: Revista de relaciones laborales*, Zaragoza, n. 2, , n. 2, p. 177-198, 1994. Disponível em: <https://dialnet.unirioja.es/descarga/articulo/229694.pdf>. Acesso em: 21 out. 2021.

UNIÃO EUROPEIA. Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. **Jornal Oficial das Comunidades Europeias**, Estrasburgo, 24 out. 1995. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:1995:281:FULL&from=PT>. Acesso em: 12 set. 2021.

UNIÃO EUROPEIA. Parecer 15/2011 sobre a definição de consentimento. **Grupo de Trabalho do Artigo 29**, Bélgica, 13 jul. 2011. Disponível em: https://www.gpdp.gov.mo/uploadfile/others/wp187_pt.pdf. Acesso em: 04 out. 2021.

UNIÃO EUROPEIA. Parecer 5/2014 sobre técnicas de anonimização. **Grupo de Trabalho do Artigo 29**, Bélgica, 10 abr. 2014. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_pt.pdf. Acesso em: 16 out. 2021.

UNIÃO EUROPEIA. Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. **Jornal Oficial das Comunidades Europeias**, Estrasburgo, 27 abr. 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=PT>. Acesso em: 12 set. 2021.

VAINZOF, Rony. Capítulo I. Disposições Preliminares. *In*: **LGPD: Lei Geral de Proteção de Dados comentada**. MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. 2. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2020. p. 22-200.

WINTER, Luís Alexandre Carta; PRIGOL, Natalia Munhoz Machado. Empresa de Tendência: um estudo comparado entre o Mercosul e a União Europeia. **Revista da Faculdade de Direito**, Porto Alegre, n. 36, ago. 2017, p. 183-206. Disponível em: <https://seer.ufrgs.br/revfacdir/article/view/73401/43559>. Acesso em: 21 out. 2021.