PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO
PUC-SP

Aimée Moraes Ribeiro Malato

ANÁLISE DA LEI GERAL DE PROTEÇÃO DE DADOS E SUAS IMPLICAÇÕES NAS RELAÇÕES TRABALHISTAS

SÃO PAULO
2021

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO
PUC-SP

Aimée Moraes Ribeiro Malato

ANÁLISE DA LEI GERAL DE PROTEÇÃO DE DADOS E SUAS IMPLICAÇÕES NAS RELAÇÕES TRABALHISTAS

Monografia apresentada à Banca Examinadora da Pontifícia Universidade Católica de São Paulo, como exigência parcial para obtenção do título de ESPECIALISTA em Direito do Trabalho, sob a orientação da Prof. Dra. Catia Guimaraes Raposo Novo Zangari.

SÃO PAULO
2021

Banca Examinadora

_____

_____

_____

Aprovada em: ___/___/___

Dedico este trabalho ao meu pai, maior jurista e professor que conheço, por sempre ter me apoiado e estado ao meu lado ao longo de minha jornada profissional, das mais variadas maneiras possíveis, tendo sido determinante para o meu crescimento pessoal e profissional.

RESUMO

A presente monografia tem por objetivo abordar os direitos do indivíduo à intimidade e privacidade previstos na Constituição Federal à luz do novo regramento apresentado pela Lei Federal nº 13.709/2018, em plena vigência desde o dia 18 de setembro de 2020, bem como analisar os seus impactos nas relações de trabalho. Para tanto, inicialmente, será apresentado um panorama geral do direito à proteção dos dados pessoais, resgatando o histórico do regramento do tema e uma comparação com Regulamento Geral de Proteção de Dados da Europa. Serão abordadas as adequações a serem observadas pelas empresas para integral e correto atendimento das previsões legais, explanando as funções do controlador, operador e encarregado, bem como os direitos dos titulares dos dados e as respectivas sanções aplicáveis na hipótese de descumprimento das obrigações emanadas pela Lei Federal nº 13.709/2018. Por fim, serão analisados os impactos da Lei Federal nº 13.709/2018 nas relações trabalhistas, inclusive na seara da responsabilidade civil e do ônus da prova no processo do trabalho, concluindo com uma análise da aplicação da Lei Federal nº 13.709/2018 pelos Tribunais Trabalhistas e sugestões para a plena compatibilidade às novas exigências legislativas.

Palavras-chave: Lei Geral de Proteção de Dados; LGPD; Relações Trabalhistas; Direito do Trabalho.

ABSTRACT

This monograph aims to address the individual's rights to intimacy and privacy pursuant to the Federal Constitution in light of the new regulation presented by Law No. 13,709 / 2018, in full force since September 18, 2020, as well as its impacts on labor relations. For this purpose, initially, a general overview of the right to the protection of personal data will be presented, retrieving the history of the regulation of the subject and a comparison with the General Regulation on Data Protection in Europe. The adjustments to be observed by the companies for full and correct compliance with the legal provisions will be addressed, explaining the functions of the controller, operator and person in charge, as well as the rights of the data owners and the respective sanctions applicable in the event of non-compliance with the obligations issued by the Law nº 13,709 / 2018. Finally, the impacts of Law No. 13,709 / 2018 on labor relations will be analyzed, including in the area of civil liability and the burden of proof in the labor process, concluding with an analysis of the application of Law No. 13,709 / 2018 by the Labor Courts and suggestions for full compatibility with new legislative requirements.

Keywords: Aplication; General Data Protection Law; LGPD; Labor relations; Labor law.

SUMÁRIO

INTRODUÇÃO 6

1. Visão geral do direito à proteção de dados pessoais 10

1.1. Considerações preliminares 10

1.2. Introdução do direito à proteção de dados no regramento jurídico na Europa e no Brasil 12

2. A Lei Geral de Proteção de Dados Pessoais nas relações trabalhistas 14

2.1. Conceitos básicos, sujeitos e objeto de regulamentação 20

2.2. Fundamentos basilares da lei 23

2.3. Hipóteses legais de não aplicabilidade da lei 25

2.4. Eficácia espacial da lei 27

2.5. Observâncias a serem feitas pelas empresas para fins de cumprimento 28

3. Situações práticas no direito do trabalho envolvendo o tratamento de dados 35

3.1. *Background checks* - Análise de antecedentes do empregado ..... **Error! Bookmark not defined.**

3.2. Utilização de dados biométricos ..... **Error! Bookmark not defined.**

3.3. Fiscalização das redes sociais do empregado 40

3.2. *Imbalance of power*. O consentimento dado pelo empregado 40

4. Sanções estabelecidas pela Lei Geral de Proteção de Dados Pessoais 42

CONCLUSÃO 47

REFERÊNCIAS 57

INTRODUÇÃO

No mundo contemporâneo, no qual as transformações socioeconômicas causadas pelo processo de metabolismo promovido pelo capitalismo ocorrem de maneira imprevisível e dinâmica, o mundo cibernético ganha cada vez mais força e influência nas relações sociais[1], apresentando inúmeras vantagens e facilidades decorrentes de seu uso ao mesmo tempo em que cria e expande uma base de dados de seus usuários com o armazenamento de informações pessoais.

A proteção de dados é um direito que nasce vinculado à Declaração Universal dos Direitos Humanos (DUDH), aprovada em 1948 pela Assembleia Geral das Nações Unidas, e que tem como objetivo garantir a dignidade da pessoa através do combate à opressão, impunidade e insultos à dignidade humana, além da invasão de privacidade que envolve a coleta e o tratamento excessivo de dados pessoais.

Não deve ser olvidado que a presente monografia está intrinsecamente ligada à tecnologia e a sua aplicação nas relações de trabalho. O avanço tecnológico no âmbito da informação e comunicação renova a forma de armazenamento dos dados pessoais dos empregados e demais colaboradores de uma empresa, se tornando cada vez mais imperativa a necessidade de observância das regras aplicáveis.

O intuito ao se promover a proteção dos dados armazenados no mundo cibernético é estabelecer uma estrutura de garantias que permita exercer os direitos e liberdades fundamentais dos seres humanos e impedir que o uso de informações pessoais seja feito de maneira indiscriminada.

Por muitos anos o armazenamento, o uso, a divulgação e a comercialização dos dados pessoais armazenados no ambiente virtual passaram sem o devido prestígio pelo

[1] Pérez Luño sustenta que: “El contexto en el que se ejercitan hoy los valores democráticos y los derechos humanos es el de una sociedad donde las Nuevas Tecnologías (NT) y las Tecnologías de la Información y de la Comunicación (TIC) y, en especial, la Red han devenido el símbolo emblemático de nuestra cultura. En el momento presente, para designar el marco de nuestra convivencia se alude reiteradamente a expresiones tales como la “sociedad de la información”, la “sociedad informatizada” o la “era de Internet”. Para las nuevas generaciones (indignadas o no), “ya está todo en la Red”. Em tradução livre, no original: "O contexto em que os valores democráticos e os direitos humanos são exercidos hoje é o de uma sociedade onde as Novas Tecnologias (NT) e as Tecnologias de Informação e Comunicação (TIC) e, especialmente, a Rede se tornaram o símbolo emblemático da nossa cultura. Atualmente, para designar o quadro de nossa convivência, nos referimos repetidamente a expressões como a "sociedade da informação", a "sociedade computadorizada" ou a "era da Internet". Para as novas gerações (indignadas ou não), "tudo está na Net". PÉREZ LUÑO, Antonio Enrique. Los derechos humanos em la sociedad tecnológica. Madrid: Universitas, 2012, pág. 41.

legislador brasileiro, iniciando um período de incertezas entre o juslaboralistas e acarretando muitas dúvidas e poucas soluções consensuais.

A primeira tentativa de mitigar a preocupação existente com questões relativas ao uso de dados pessoais no Brasil se deu com a criação da Lei Federal nº 12.965/2014, também conhecida como "Marco Civil da Internet", o qual previu, em seu artigo 7º, que o acesso à internet é essencial ao exercício da cidadania.

Alguns anos após, também demonstrando uma preocupação com a necessidade de um regulamento específico e criterioso diante do avanço da tecnologia, a União Europeia aprovou o Regulamento Geral de Proteção de Dados da União Europeia ("GDPR"), cujo objetivo principal é fornecer aos indivíduos o controle sobre seus dados pessoais e simplificar o ambiente regulatório para negócios internacionais na medida em que unifica a regulamentação sobre o assunto na União Europeia.

Em vigor desde maio de 2018, a GDPR promove uma regulamentação de dados pessoais na União Europeia e no Espaço Econômico Europeu, tratando também da transferência desses dados pessoais para fora desses espaços, tendo se tornado um marco inovador e importante para o direito digital, servindo de modelo para muitos outros países reforçarem suas políticas pré-existentes.

A entrada em vigor da GDPR ocorreu em um período em que as autoridades e os legisladores brasileiros buscavam respostas para as questões relativas à segurança virtual, a qual ganhava cada vez mais atenção diante do aumento exponencial dos crimes cibernéticos. Um estudo realizado pela empresa de segurança digital *McAfee* e publicado na revista *Veja* em 21 de fevereiro de 2018[2] revelou que o Brasil registrou perdas progressivas com crimes virtuais, chegando a US$ 10 bilhões de dólares (R$ 32,4 bilhões de reais[3]) por ano, tornando o país uma "potência" do crime virtual, ao lado de Rússia, Coreia do Norte, Índia e Vietnã.

Seguindo o respaldo jurídico europeu dado à temática, em 14 de agosto de 2018 o presidente Michel Temer sancionou a Lei Federal nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados ("LGPD"). Com origem no Projeto de Lei Complementar nº 53/2018, aprovado por unanimidade e em regime de urgência pelo Plenário do Senado em julho de 2018, a norma tem como propósito dispor sobre o tratamento de dados pessoais, por pessoa

[2] https://veja.abril.com.br/economia/brasil-perde-us-10-bilhoes-por-ano-com-cibercrime-diz-mcafee/. Acesso em: 13 de janeiro de 2021.
[3] Valor referente ao ano de 2018.

natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural[4].

Em pleno vigor e de observância obrigatória desde o dia 18 de setembro de 2020, a LGPD surgiu como um desafio para as empresas que lidam com dados pessoais, trazendo uma série de regras cuja integral conformidade servirá como divisor entre empresas que apresentarão uma vantagem competitiva, aumentando o nível de confiança de seu público, e empresas que sofrerão as sanções administrativas aplicadas pela Autoridade Nacional de Proteção de Dados ("ANPD").

Sobre o que se trata o direito à proteção de dados pessoais? O que é a LGPD? Como ela surgiu? Quais foram as suas fontes de inspiração no direito comparado? Quais as principais fontes materiais que levaram à sua criação? Quais são os regramentos previstos na lei? De que forma a LGPD impacta nas relações de trabalho? Qual a responsabilidade civil do empregador decorrente da ofensa dos direitos protegidos pela LGPD? Essas e outras perguntas tentarão ser paulatinamente respondidas no desenvolvimento do presente trabalho, o qual, embora não tem a intenção de esgotar o assunto, conta com estudos jurídicos, doutrinas e análises práticas sobre a LGPD no direito do trabalho.

No primeiro capítulo será discutida a visão geral do direito à proteção de dados, repassando o histórico que levou ao surgimento deste novo plexo de direitos fundamentais integrantes da quinta dimensão, intimamente relacionados com as repercussões sociais e jurídicas da internet. Em seguida, será analisado de que forma esses direitos passaram a ser regulamentados no âmbito jurídico internacional[5].

Dando andamento ao trabalho, no segundo capítulo é trazida em pauta a introdução da LGPD no ordenamento jurídico brasileiro, sempre alicerçado em sua relação com o direito do trabalho e seus impactos nas relações trabalhistas.

No terceiro capítulo, a LGPD é encarada mais a fundo no contexto das relações de trabalho, bem como questões práticas da aplicação da norma. Finalmente, o quarto capítulo terá como objetivo analisar a atuação da ANPD como órgão fiscalizador, discutindo as

[4] Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

[5] BEPPLER, Daniela. Internet e informatização: implicações no universo jurídico. In: ROVER, A. J. (Org.). Direito, sociedade e informática: limites e perspectivas da vida digital. Florianópolis: [s.n.], 2000, Pág. 121.

sanções e penalidades trazidas pelo legislador brasileiro para as empresas que não se adequarem às novas regras.

1. Visão geral do direito à proteção de dados pessoais

Neste primeiro momento, serão analisadas as premissas básicas envolvendo o direito à proteção de dados pessoais e de que forma esse direito passou a ser introduzido no regramento jurídico internacional e nacional, com o objetivo a criar uma base para posterior análise de sua implicação no direito do trabalho e nas relações trabalhistas.

1.1. Considerações preliminares

A nova gama de direitos fundamentais integrantes da quinta dimensão, os quais se relacionam intimamente com as repercussões sociais e jurídicas da internet, surgem dentro de um universo que apresenta novos meios, ambientes, processos e tecnologias de informação, constituindo processos de empoderamento e conferindo visibilidade e voz aos que não as tinham[6].

O mundo, em constante modificação oriunda do avanço tecnológico, muda substancialmente a vida das pessoas em diferentes níveis, acarretando a criação de categorias de direitos que podem ser divididas de duas formas: a primeira, envolvendo a necessidade de proteção em face de riscos à dignidade, igualdade e liberdade que derivam do mundo cibernético; e a segunda, envolvendo as condições de ampliação e promoção dos direitos pelas vias que são propiciadas por esse mundo cibernético, objetivando evitar práticas discriminatórias e preconceituosas, como manifestações de discurso do ódio.

É dentro dessa realidade de transformações causadas pela globalização e disseminação de conteúdo entre indivíduos que nasceu a imperiosa necessidade de se tutelar a quinta dimensão de direitos fundamentais, representados pelos avanços da era digital.

O mundo cibernético tem possibilitado cada vez mais a extração de dados, de forma massiva, de seus usuários. Os dados obtidos, reunidos e processados em uma enorme quantidade em questão de segundos, permite que aquele que os tem em seu poder possa usá-lo, repassá-los e comercializá-los, inclusive influenciando condutas em níveis até hoje desconhecidos.

---

[6] CONI JR, Vicente Vasconcelos. A cibercidadania como consequência de um novo modelo de governança da gestão de políticas púbicas. Florianópolis. Empório do direito. 2019. Pag. 117

A cada ano, milhões de consumidores entram nas 1.147 lojas da Target existentes e fornecem terabytes de informações sobre si mesmos sem nem mesmo ter consciência disso. A partir dessas informações prestadas, os analistas da Target são capazes de prever o que está acontecendo em suas vidas e, mais do que isso, rastrear de perto os hábitos – no caso, de compras – dessas pessoas.

Embora alguns dos métodos utilizados para rastrear informações de seus usuários ainda se revelem "à moda antiga" – utilização de cartão fidelidade, cartão de crédito, troca de cupons etc. -, atualmente as empresas vão além: a partir um vasto armazém de dados construído com informações prestadas pelos usuários, torna-se possível saber muito mais do que apenas o que o indivíduo gostaria ou permitia que se soubesse.

Observa-se, portanto, que, sem uma regulamentação acerca do assunto, os dados pessoais fornecidos pelos usuários ou deles extraídos passam a constituir uma espécie de ativo comercial das grandes empresas – e não só de tecnologia - espalhadas pelo mundo, com o claro objetivo de obtenção de capital.

Os dados pessoais passaram, portanto, a possuir extrema relevância, nos mais diversos aspectos, diante do poder e alcance inimagináveis das tecnologias digitais de comunicação[7].

Em paralelo, surge também a necessidade de se resguardar o exercício dos direitos fundamentais, notadamente os direitos à privacidade e intimidade.

O direito à privacidade, previsto na Constituição Federal como um direito à vida privada, busca proteger o indivíduo de invasões de terceiros na sua esfera íntima e pessoal, compreendendo aqui o seu lar, a sua família, sua correspondência e até mesmo aspectos negociais.[8]

Esse direito do ser humano à privacidade vem assumindo, de fato, maior relevo, como observado por Carlos Alberto Bittar em seu livro "Os direitos da personalidade":

> "Esse direito vem assumindo, paulatinamente, maior relevo, com a contínua expansão das técnicas de virtualização do comércio, de comunicação, como defesa natural do homem contra as investidas tecnológicas e a ampliação, com a necessidade de locomoção, do círculo relacional do homem, obrigando-se à exposição permanente perante públicos os mais distintos, em

[7] Castells, inclusive pontua que "a participação no âmbito virtual poderá levar a redistribuição do poder e também com exercício de um direito no contexto mais amplo da cidadania". CASTELLS, M. A sociedade em rede. A era da informação: economia, sociedade e cultura. Tradução Roneide Venâncio Majer. São Paulo: Paz e Terra, 2016. v.1.

[8] BITTAR, Carlos Alberto. Os direitos da personalidade. São Paulo. Saraiva. 8 ed. 2015. pág. 172/173.

> seus diferentes trajetos sociais, negociais ou de lazer. É fato que as esferas de intimidade têm-se reduzido com a internet e meios eletrônicos."[9]

Da mesma forma, a necessidade de proteção desta categoria de direitos fundamentais se revela necessária diante da existência de um novo modelo social baseado no chamado capitalismo de vigilância, característico por adotar uma nova lógica de acumulação, com uma nova política e relações sociais que substituem os contratos. Maurício Requião pontua:

> O mundo, especialmente ao longo da última década, foi moldado para extrair dados dos usuários da Internet em escala massiva. Estes dados, reunidos e processados através do que se convencionou chamar de Big Data, que permite a obtenção de informações e o poder de influenciar condutas, em escalas até o presente momento ainda não inteiramente esclarecidas. Assim, os dados pessoais são transformados em importante ativo comercial das grandes empresas de tecnologia do mundo, com o claro objetivo de obtenção de capital, além de outros até o momento não tão claros assim.

Embora a coleta de informações não seja, como já visto, decorrente única e exclusivamente da sociedade da informação[10], a sua relevância e preocupação jurídica atual se dá devido à crescente velocidade da coleta e manipulação de dados, atividades que muitas vezes não estão nem mesmo na esfera de conhecimento dos cidadãos.

Sobre o assunto, SARLET leciona:

> Embora não se trate de direito absoluto, o direito à proteção dos dados, especialmente na medida de sua conexão com a dignidade humana, revela-se como um direito bastante sensível, tanto mais sensível quanto mais a sua restrição afeta a inti midade e pode implicar violação da dignidade da pessoa humana (SARLET; MARINONI; MITIDIERO; 2018, p.497).

Em 1890 foi publicado na "Harvard Law Review" o ensaio acadêmico nomeado "The right to privacy", escrito por Samuel D. Warren e Louis D. Brandes[11]. Desde então considerado um marco doutrinário sobre o direito à privacidade, o estudo demonstrou, já à

[9] BITTAR, Carlos Alberto. Os direitos da personalidade. São Paulo. Saraiva. 8 ed. 2015. pág. 173.
[10] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. In: Espaço Jurídico, Joaçaba, v. 12, n. 2, jul./dez. 2011, p. 92.
[11] WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. In: Harvard Law Review, vol. 4, nº 5 (Dec. 15, 1980), p. 193-220.

época, a preocupação com os impactos das novas tecnologias nas esferas menos penetráveis da vida de cada pessoa[12].

Na medida em que avança a capacidade de armazenar, tratar e comunicar as informações, aumentam as formas de utilização dos dados pessoais, os quais passam a poder ser utilizados não apenas de forma lícita, mas em total desrespeito e violação ao direito à privacidade do usuário.

É diante desses avanços tecnológicos que os legisladores, observando que a proteção jurídica não mais se revelava suficiente para resguardar o direito à privacidade/intimidade, começaram a se debruçar sobre o tema com o objetivo de regular a proteção de dados pessoais até chegar à criação da LGPD, conforme será debatido a seguir.

1.2. Introdução do direito à proteção de dados no regramento jurídico na Europa e no Brasil

A sociedade moderna foi, indubitavelmente, transformada com a chegada e consolidação da chamada era digital das tecnologias da informação e da comunicação a ponto de ser impossível mensurar os limites e o real alcance no futuro da comunidade mundial.

O universo constituído de rede de computadores, meios, ambientes, processos e tecnologia de informação desafiam o resguardo dos direitos fundamentais, frente aos riscos à dignidade, igualdade e liberdade que derivam desse globalizado mundo cibernético, uma vez que a crescente capacidade de armazenamento e comunicação de informações aumenta a possibilidade de coleta desses dados para fins lícitos, mas também com viés contrário àquele pretendido pelo titular do fornecimento do dado.

Para fazermos uma análise acerca da introdução da proteção de dados pessoais no ordenamento jurídico brasileiro, faz-se necessário pesquisar de que forma essa introdução

[12] A seguinte passagem bem ilustra a preocupação dos autores: "Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right 'to be let alone (Cooley on Torts, 2. ed., p. 29)'. Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from house-tops'" (WARREN, Samuel D.; BRANDEIS, Louis D. op. cit., p. 195. Em tradução livre: Recentes invenções e métodos de negócios chamam a atenção para o próximo passo que deve ser dado para a proteção da pessoa e para garantir ao indivíduo o que o juiz Cooley chama de direito de direito de "ser deixado sozinho" (Cooley on Torts, 2. ed., p. 29). Fotografias instantâneas e empresas de jornais invadiram os recintos sagrados da vida privada e doméstica; e inúmeros dispositivos mecânicos ameaçam retificar a previsão de que "o que é sussurrado no armário deve ser proclamado do topo da casa".

ocorreu no ordenamento europeu, por ter servido de inspiração para o sistema brasileiro de proteção de dados (PECK, p.16, 2018).

A ascensão da tecnologia e os impactos na informação e dados pessoais foi muito bem debatida por DANILO DOEDA (2000):

> Foi na década de 60 que juristas europeus e norte-americanos começaram a vislumbrar o potencial de dano representado pela informatização de informações pessoais. Na década seguinte, começaram a surgir os primeiros meios de proteção, de acordo com a visão tecno-cultural da época, tendo como referencial os modelos de difusão de informações dos meios culturais de massa. Este modelo pressupunha a oferta de informações, realizada por grandes centros de difusão que se dirigiam à periferia em um caminho de mão única.
> Entendia-se que a legislação de proteção de dados pessoais deveria observar este estado de coisas, onde poucos e gigantescos centros elaboradores de dados dominariam o fornecimento de informações e a gestão dos grandes bancos de dados; portanto, a ofensa à privacidade viria necessariamente destes grandes centros. Foram elaboradas leis com este fim, conhecidas pelos autores como leis "de primeira geração" sobre o tratamento automático de informação. (DONEDA, 2000, p. 15).

A fim de tutelar o direito à privacidade dos indivíduos, muitos e relevantes avanços na seara normativa foram produzidos, especialmente na Europa, no que se refere à busca pelo amparo à privacidade e intimidade da pessoa. E o resguardo à proteção de dados não ficou à margem dessa discussão.

As “leis de primeira geração”, mencionadas por Danilo Doeda (2000), logo se revelou ineficaz diante do avanço crescente multiplicação dos centros de processamento, levando à necessão de adoção de outros instrumentos e iniciativas na área.

A Organização para a Cooperação e Desenvolvimento Econômico (OCDE) e o Conselho da Europa criaram em 1980 e 1981 respectivamente, dois instrumentos na área, nomeados Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais e a Convenção nº 108/1981.

O primeiro teve como objetivo estabelecer diretrizes não obrigatórias para proteção e coleta de dados aos países-membros da OCDE para incluírem em seus ordenamentos jurídicos, conforme explicado por Roberto Ribeiro de Britto[13].

Com relação à Convenção nº 108/1981, por sua vez, explica RODRIGUEZ que se trata do “primeiro texto jurídico unificado sobre a matéria, que se propôs a garantir no

[13] (BRITTO; RIBEIRO, 2018, p. 387). As Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais estão disponíveis em: http://www.oecd.org/sti/ieconomy/15590254.pdf

território de cada país-membro, o respeito aos diretos e liberdades fundamentais de todas as pessoas, independentemente de suas nacionalidades ou residências.”.[14]

Após essa “segunda geração” de leis, como chamado por DANILO DOEDA (2000), surgiu a “terceira geração” de leis, que refletiu a proliferação dos bancos de dados e a necessidade de uma tutela que se revelasse mais flexível e que se mostrasse atenta à dinâmica inerente ao avanço tecnológico.

A Alemanha foi pioneira em reconhecer o direito à proteção de dados, em julgamento realizado pelo Tribunal Constitucional Alemão, no ano de 1982, no caso da Lei do Censo Alemã[15].

Tal lei autorizava a excessiva coleta de dados quando da realização do censo demográfico disponibilizando-os ao estado, com o objetivo fim de execução administrativa. O tribunal julgou inconstitucional a abrangência e uso dessa coleta, entendendo que o direito à audoterminação informativa “pressupõe que, mesmo sob as condições da moderna tecnologia de processamento de informações [...] o indivíduo exerça sua liberdade de decisão sobre as ações a serem precedidas ou omitidas em relação a seus dados”. (VIEIRA, 2007, p.88).

E o Tribunal foi além em sua decisão. Baseado no direito geral da personalidade consagrado na *Grundgesetz* reconheceu que:

> “o livre desenvolvimento da personalidade pressupõe, sob as modernas condições do processamento de dados, a proteção do indivíduo contra levantamento, armazenagem, uso e transmissão irrestritos de seus dados pessoais, assegurando, assim, a proteção à autodeterminação informativa”.

Como se vê, a discussão, em esfera jurídica, a respeito da temática proteção de dados pessoais, não é nova. Remonta, certamente, à década de 1970, período em que países como Alemanha, Suécia, Dinamarca, Noruega e França deram o pontapé inicial na regulamentação da matéria, emoldurado um modelo europeu consolidado com a Diretiva 95/46/CE[16] do Parlamento Europeu e do Conselho, que é o texto de referência em matéria de proteção dos dados pessoais.

---

[14] (RUARO; RODRIGUEZ, 2010, p. 167-168). A Convenção nº 108/1981 está disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.

15 MOREIRA, Teresa Coelho. A Privacidade dos Trabalhadores e as Novas Tecnologias de Informação e Comunicação: Contributo para um estudo dos limites do poder de controlo electrónico do empregador. Coimbra: Almedina, 2010.

16 (DONEDA, 2006). A Diretiva nº 95/46/CE está disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=PT.

A Diretiva 95/46/CE marcou o direito comunitário europeu, ao estabelecer o dever dos Estados de criarem códigos de condutas nacionais e comunitários para dar maior efetividades às suas disposições. Como explica DANILO DOEDA (2000), a Diretiva acentuou que a proteção dos dados pessoais deveria ser aplicada tanto na hipótese de tratamento automatizado como na de tratamento manual, da mesma forma que a observância de suas determinações deveria se dar tanto pelo setor público quanto pelo setor privado.

A partir desta diretiva, os países europeus começaram a providenciar a criação de leis próprias de proteção de dados. Danilo Doeda (2000) refere que inclusive países excluídos do grupo de liderança em tecnologia, como Portugal, passou a prever em sua Constituição meios jurídicos para proteção de dados pessoais.

No ano de 1997 foi criada nova Diretiva, nº 97/66/CE[17], posteriormente revogada e substituída pela Diretiva nº 2002/58/CE, que tratava acerca do tratamento de dados pessoais pessoal e da proteção à intimidade relacionado ao setor de telecomunicações. Em 2006, sobreveio a Diretiva 2006/24/CE tratando acerca da conservação de dados gerados e tratados em uma relação de oferta de serviços de comunicações eletrônicas publicamente disponíveis ou de redes públicas de comunicações.

Em 2016, o Parlamento Europeu aprovou o Regulamento Geral de Proteção de dados Pessoais da União Europeia (RGPD), que entrou em vigor a partir de 25 de maio de 2018, servindo esse de luz inspiradora para a criação da Lei Geral de Proteção de Dados (LGPD).

A RGPD se revela como a mais importante norma que trata da proteção de dados, instituída em substituição à Diretiva 95/46/CE, mas que se manteve, na visão de SCHREIBER, "fiel à tradição europeia de efetiva preocupação com a questão da privacidade e da proteção de dados, significando não uma ruptura com o sistema anterior, mas sim seu aprofundamento."

Tal como a Convenção nº 108/1981, a RGPD define dados pessoais, em seu artigo 4º, item 01, como:

> Informação relativa a uma pessoa singular identificada ou identificável ('titular dos dados'); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental,

[17] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31997L0066&from=PT.

> económica, cultural ou social dessa pessoa singular; (UNIÃO EUROPEIA, 2016).

GIMÉNEZ (2019, p. 06) analisa a norma e destaca como sendo uma novidade a inclusão de novas formas de identificar uma pessoa devido a avanços tecnológicos e sua aplicação no ambiente empresarial. Menciona ainda, como exemplos em uma relação trabalhista, a impressão digital como mecanismo de controle da pontualidade dos empregados.

Em âmbito nacional, anteriormente à promulgação da LGPD, apenas legislação esparsa[18] poderia socorrer a proteção aos dados pessoais, tendo como sustentáculo o artigo 5°, incisos, X, XI e XII, da CF; artigos 20 e 21, do Código Civil; artigo 201, § 6°, do Código de Processo Penal; artigos 43 a 45 da Lei n° 8.078/1990 (CDC); Lei n° 9.507/1997 (Habeas Data); Lei n° 12.527/2011 (LAI); e a Lei n° 12.965/2014 (Marco Civil da Internet).

Há de se destacar a importância de duas propostas de Emenda Constitucional que trazem grandes mudanças no ordenamento jurídico brasileiro em relação ao acesso igualitário aos meios digitais assim como uma proteção maior aos dados pessoais. São elas a PEC 185/15, aprovada pela Comissão de Constituição e Justiça, que inclui o direito de acesso à internet na categoria de garantias fundamentais ao cidadão, e a PEC 17/2019, que acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal, para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Para Pamplona Filho (2020, p. 6):

> De fato, a proteção jurídica do direito à privacidade/intimidade até determinado momento histórico se mostrava em alguma medida suficiente, mas hoje com o desenvolvimento da informática, armazenam-se um número ilimitado de dados de todas as naturezas, os quais circulam entre Estados, particulares e empresas privadas, muitas vezes sem qualquer tipo de controle, fica clara a necessidade de maior proteção.

Não há como olvidar, quando feita a análise dos fatores que impulsionaram a edição da LGPD, casos como o vazamento ou uso indevido de dados pessoais para fins de manipulação eleitoral e política, fartamente noticiado pela imprensa nacional e internacional (referência clara à Cambridge Analytica) ou mesmo o isolamento jurídico em que o Brasil se encontrava, face ao panorama internacional, por não dispor de uma legislação específica de proteção de dados pessoais.

---

[18] SORIANO, Olga Fuentes. La prueba prohibida. Viejos problemas procesles de las nuevas tecnologias. In PRIORI POSADA, Giovanni. Justicia y proceso en el siglo XXI. Desafios y tareas pendientes. Lima. Palestra Editores, 2019. Pág. 389-416.

A LGPD, portanto, é a lei vestibular brasileira que normatiza a proteção aos dados pessoais, e que vem estabelecer os princípios norteadores dos diretos básicos referentes à matéria, além de abarcar os fundamentos e obrigações impostas aos responsáveis por controlar tal proteção.

2. A Lei Geral de Proteção de Dados Pessoais nas relações trabalhistas

Objetivando alinhar-se ao cenário mundial que se movimentava em busca de uma melhor proteção de dados pessoais, o legislador brasileiro editou a LGPD, cuja entrada em vigor se deu em agosto de 2020.

A LGPD, revelando uma inequívoca transversalidade, impacta direta ou indiretamente todas as áreas do direito e tem como objetivo principal proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, conforme se observa de seu artigo 1º:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Além da proteção à pessoa humana, objetivo expressamente exposto no artigo 1º, é inconteste que a escolha do legislador brasileiro ao editar a LGPD também se deu por razões de ordem econômica, caracterizadas através da tentativa de se evitar o isolamento das empresas brasileiras do mercado geral e perdas de competitividade e de investimentos estrangeiros.

Essa preocupação é estampada no relatório elaborado pelo senador Ricardo Ferraço, no qual aduz que a edição de uma lei geral de proteção de dados se revelava imprescindível tendo em vista que o país estaria perdendo oportunidades valiosas de investimento financeiro internacional em razão do isolamento jurídico em que se encontrava por não dispor de uma lei que tratasse dessa questão.

Nesse sentido observa Tarcísio Teixeira e Ruth Maria Armelin (2019, p. 26):

> Os dados pessoais são considerados o novo petróleo da sociedade informacional, a base de um gigantesco mercado, já que através deles é

> possível identificar perfis de consumo, potencialidades de mercado, além de inúmeras outras possibilidades, altamente lucrativas.

De fato, desde a data de vigência da GDPR, principal norma de proteção de dados da União Europeia, as empresas europeias ficaram, de certa forma, impedidas de fechar negócios com empresas situadas em países que não dispunham de um nível de proteção adequado, o que incluía o Brasil.

É justamente em decorrência desse caráter transversal que a LGPD impacta nas relações de trabalho, as quais se caracterizam pela desigualdade fático-jurídica entre os contratantes e, ainda, por uma relação contratual em que o objeto do contrato – salário – se revela essencial para a sobrevivência de um desses contratantes.

Em que pese a LGPD não seja expressa em seu texto legal acerca de suas aplicações nas relações trabalhistas, é inconteste o seu alcance sobre a proteção de dados dos empregados, já que a lei objetiva proteger os dados da pessoa natural, o que inclui a pessoa do empregado.

A relação naturalmente conflituosa e estruturalmente assimétrica que se observa entre empregado e empregador é regulada, como se sabe, pelo Direito do Trabalho, o qual tutela os direitos dos trabalhadores de forma a compensar essa debilidade fática por eles apresentada.

Não há qualquer dúvida acerca da aplicação da proteção dos direitos fundamentais do empregado na relação privada existente em uma relação trabalhista, o que torna ainda mais evidente a aplicação da LGPD como uma forma de proteção aos direitos fundamentais dos empregados nas relações trabalhistas, em especial do direito ao livre desenvolvimento da personalidade, do qual decorrem a proteção da intimidade, da privacidade e da autodeterminação informativa (também denominado direito à privacidade decisional e informacional).

Para conseguir se entender de que forma a LGPD impacta as relações de trabalho, é necessário tão somente imaginarmos o enorme fluxo de dados de titularidade dos trabalhadores que circula no âmbito de uma empresa desde a entrevista de admissão até a rescisão contratual – ou até mesmo depois disso.

A LGPD é, “na grande maioria das vezes, expressão de um direito do empregado e portanto, o tratamento de dados no contexto laboral é, via de regra feito, em favor do

empregado[19], e na defesa dos seus interesses, sendo portanto, uma obrigação do empregador.".[20]

Com a chegada da nova lei, é imprescindível que o empregador tome conhecimento de seus deveres e obrigações, bem como quais dados podem ou não ser por ele armazenados. Na realidade, nem mesmo basta que se faça o correto enquadramento da situação à hipótese legal prevista na LGPD, mas também saber o modo pelo qual o tratamento poderá ser realizado, isto é, por quanto tempo, em qual lugar e de que forma ou procedimento.

Por óbvio, não se pode partir da equivocada premissa de que as relações trabalhistas são absolutas. Justamente por não serem é que se torna necessário analisar caso a caso, sendo plenamente possível nos depararmos com restrições diante das peculiaridades e exigências de um contrato de trabalho específico.

Em se tratando do período **pré-contratual** de uma relação trabalhista e a atenção quanto à proteção de dados, deverá despertar o cuidado do empregador os chamados "background checks", isso é, a investigação da vida privada do trabalhador. Inclui-se aqui, entre outros, pesquisa acerca dos precedentes de crédito, solicitações de certidão de antecedentes criminais e pedidos de referência e bons antecedentes funcionais a outros empregadores, o que, inclusive deve gerar a "revisão por parte dos recursos humanos quanto aos processos seletivos, para contratação laboral, especialmente quanto ao tipo de informações/dados requisitados aos candidatos, especialmente aqueles considerados sensíveis"[21].

Também deverá ser adotado, por parte do empregador, o procedimento correto para a adequada coleta de dados "não sensíveis" e "sensíveis" nas entrevistas de emprego, como, por exemplo, o acesso ao patrimônio genético do empregado; perguntas sobre dados relacionados à convicção religiosa, opinião política, filiação sindical ou a organizações de caráter religioso, filosófico ou político; e dados relacionados à saúde ou à vida sexual.

É necessário ter cautela, sobretudo, no que tange a dois dos princípios da LGPD, quais sejam, a não discriminação e a finalidade. Com relação ao primeiro, a vedação é dada

---

[19] MIZIARA, Raphael. LGPD: razões de sua existência e impactos nas relações de emprego. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/lgpd-razoes-de-sua-existencia-e-impactos-nas-relacoes-de-emprego-15032020 Acesso em: 22 de março 2021.

[20] OLIVIERI, Nicolau. LGPD e sua necessária adequação às relações de trabalho. Disponível em https://www.jota.info/opiniao-e-analise/artigos/lgpd-e-sua-necessaria-adequacao-as-relacoes-de-trabalho-28092019 Acesso em 13 de janeiro de 2021.

[21] REANI, Valéria. O impacto da lei de proteção de dados brasileira nas relações de trabalho. Disponível em: https://www.conjur.com.br/2018-set-21/valeria-reani-alei-protecao-dados-relacoes-trabalho Acesso em: 12 de março de 2021.

inclusive pela legislação pertinente ao tema, conforme explicam Carlos Augusto Pinto de Vasconcellos Junior e Victor Silva Ferreira (2020, s.p):

> A LGPD, em sintonia com outras legislações, como exemplo com a Lei n. 9.029/1995, prevê que não é possível haver discriminação, inclusive no momento pré-contratual. Então, os recrutadores deverão avaliar a adequação da vaga aos candidatos, de forma objetiva, sem que peçam ou busquem, ainda que informalmente, dados que possam discriminar os pretensos trabalhadores.

Com relação ao princípio da finalidade, significa dizer, entre outras coisas, que deve existir um motivo válido e pertinente para que a manutenção dos dados pessoais compartilhados pelo empregado e compartilhamento com terceiros, como por exemplo nos casos de justa causa, eis que tal informação pode acarretar prejuízos ao trabalhador no mercado de trabalho (BOLDRIN; CORREIA, 2020, s.p).

É ainda necessário saber como realizar o tratamento dos dados dos indivíduos que, participando do processo seletivo, não foram selecionados para a contratação.

A LGPD dispõe que dado pessoal "sensível" é todo 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. Vejamos, nesse sentido, o seu artigo 5º, inciso II:

> Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> 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;

Como se observa, a LGPD não conceitua o dado sensível, e sim apresenta um rol exemplificativo de dados que podem ser entendidos como tal. Em uma análise aos dados ali elencados, é possível se defender que, então, dado sensível é todo aquele dado distintivo capaz de permitir uma identificação e que, por isso mesmo, pode render ensejo a tratamentos discriminatórios em determinados contextos.

Embora o dado "gênero" não tenha sido incluído no rol elencado no artigo 5º, inciso II, da LGPD, e, portanto, a rigor, não seja considerado dado "sensível", é até mesmo evidente que, a depender do contexto, possa vir a ser considerado dessa forma. É o caso, por exemplo, do empregado que apresenta um documento de identificação com nome masculino (i.e., Mário) e preenche a ficha de cadastro para participação em entrevista de emprego com seu nome social (Maria).

Observa-se na hipótese em questão que o dado "gênero" configura um dado sensível, relacionado à orientação sexual, de forma que redobrados devem ser os cuidados despendidos por parte do empregador, sobretudo, mas não somente, durante esse período pré-contratual[22].

Durante o **período contratual**, os cuidados relacionados à proteção de dados do empregado, embora sejam outros, são igualmente importantes. Cita-se, exemplificativamente, os dados insertos nos Atestados de Saúde Ocupacional (ASO) admissionais, ou a foto do empregado que será inserida em crachá corporativo, os quais deverão ter procedimentos diferenciados.

Da mesma forma, procedimentos específicos deverão ser observados para a coleta, armazenamento e uso de informações cadastrais do empregado, tais como CPF, PIS, CTPS e filiação sindical.

Também passa a ser necessário ter em mente e observar as hipóteses legais autorizadoras para a coleta de dados biométricos (impressão digital, geometria da mão, reconhecimento facial, leitura biométrica de íris e retina)

O tratamento de dados atinentes à vida extralaboral da vida do trabalhador e monitoramento de redes sociais, correio eletrônico e de chamadas telefônicas também poderá ser realizado pelo empregador durante o período contratual, desde que de forma excepcional e corretamente enquadrada em uma das hipóteses legitimadoras previstas na LGPD.

O mesmo corre com as demais condutas como controle via sistemas de geolocalização, videovigilância ou gravação sonora; forma de coleta e armazenamento de atestados médicos, testes antidoping e de gravidez.

No **período pós contratual**, passa a ser imprescindível que o empregador saiba como se portar em relação aos pedidos de referência e de bons antecedentes funcionais formulados por outras empresas, bem como de que modo e por quanto tempo poderá

[22] AGUIAR, Antonio Carlos. **A proteção de dados no contrato de trabalho**. Revista Ltr: legislação do trabalho, São Paulo, SP, v. 82, n. 6, p. 655-661, jun. 2018.

armazenar dados de um ex-empregado. As cautelas se aplicam, ainda, no que tange ao armazenamento de dados de empregados falecidos.

Além das obrigações decorrentes das imposições legislativas, é possível que o empregador se recuse a eliminar de sua base de dados os dados fornecidos pelo empregado, principalmente durante o prazo prescricional de 02 (dois) anos (Artigo 11 da CLT), para eventuais defesas uma reclamação trabalhista, como menconado por Leandro Sampaio Correa de Araújo, para os casos que nos quais "envolvam doenças e/ou acidentes, pois o marco prescricional tem como ponto de partida o efetivo conhecimento do titular (diagnóstico e extensão dos danos) ou quando do evento morte (titular), sendo os herdeiros menores, caso em que não é deflagrado de imediato o prazo prescricional".[23]

Como explanam Raíssa Fabris de Souza e Luiz Fernando Bellinetti (2019, p. 13), é preciso "apontar a vedação de divulgação de "listas negras", sejam aquelas que apontam empregados que entraram com ações trabalhistas ou as relativas àqueles que possuem atuação sindical significativa.".

A LGPD também norteia a forma que poderá se dar o compartilhamento de dados pessoais de trabalhadores entre empresas do mesmo grupo econômico, entre empresas e entidades sindicais e, ainda, entre empresas empregadoras e empresas de planos de saúde.

Os empregados considerados hipersuficientes nos termos do artigo 444, parágrafo único, da CLT, possuem tratamento diferenciado pela LGPD, assim como empregados crianças e adolescentes (nos casos em que permitido o labor) e empresas multinacionais, tendo em vista que, neste último caso, estaríamos diante de uma transferência internacional de dados.

Como visto, a LGPD transforma as relações de trabalho e obriga o empregador, chamado pela lei de "Controlador", a submeter-se às hipóteses legais que autorizam o tratamento de dados "sensíveis" e/ou "não sensíveis" no âmbito das relações trabalhistas, assim como dispõem os artigos 7º a 11º da LGPD.

De fato, existe uma enorme possibilidade quando estamos falando de tratamento e circulação de dados pessoais no âmbito de uma relação trabalhista, "não apenas aqueles armazenados eletronicamente, mas também as informações pessoais disponíveis em qualquer mídia capaz de registrá-las, as quais estão, por iguais, sujeitas à proteção prevista na lei" (SOUZA, 2019).

---

[23] ARAÚJO, Leandro Sampaio Correa de. Impactos da Lei Geral de Proteção de Dados nas relações de trabalho Disponível em: https://www.conjur.com.br/2020-mar-14/leandro-araujo-impactos-lgpd-relacoes-trabalho Acesso em: 08 de dezembro de 2020.

Tão importante quanto saber o correto enquadramento da situação à hipótese legal que autoriza o tratamento dos dados pessoais é entender de que forma esse tratamento poderá ser realizado (tempo, lugar e forma). A LGPD não se quedou omissa quanto a isso, dispondo, em seu artigo 9º, acerca da necessidade de o empregador informar adequadamente os seus trabalhadores sobre os detalhes do tratamento de seus dados, os quais deverão ser disponibilizados de forma clara e especificando como a informação será tratada e o porquê de o tratamento ser necessário.

A prova da devida informação fornecida pelo empregador é dele, de forma que, conforme será visto, é altamente recomendado que a forma de obter o consentimento do titular seja feito de maneira mais clara do que como é feito na maioria dos casos[24].

Como exemplo prático no cotidiano das relações de trabalho, podemos citar a entrega de atestados médicos que contenham a indicação de uma doença. É claro que o trabalhador possui o direito de que a informação sobre seu estado de saúde não seja compartilhada entre os empregados até mesmo pelo elevado potencial discriminatório. Entretanto, por outro lado, a empresa tem o dever de guarda da documentação de seus empregados até para fins de reflexos previdenciários.

É fundamental, assim, que a empresa esteja preparada para criar rotinas seguras. Os atestados médicos devem ser armazenados em setor específico de segurança e medicina ocupacional (NR 04), mas esse procedimento deve ser feito com proteção adequada para não incorrer em violação à privacidade.

Para a guarda segura, caberá às empresas se adaptarem e criarem formas de tratamento para esses tipos de dados visando a proteger a privacidade de seus clientes, empregados, consumidores e prestadores de serviço, de modo que suas informações pessoais e consideradas sensíveis não sejam inadequadamente expostas, sendo possível citar como possibilidade o armazenamento digital com a utilização de criptografia.

Nesse sentido pontua a autora Laura Schertel:

> "A proteção dos dados pessoais se insere na sociedade de informação como uma possibilidade de se tutelar o indivíduo diante dos potenciais riscos que o tratamento de dados poderia causar à sua personalidade, pois o que se visa

[24] YOSHIDA, Victoria Melo. Autodeterminação informativa, riscos cibernéticos e proteção de dados pessoais: a emergência de um novo compliance. In Revista do curso de direito da Unifacs. Porto Alegre. Paixão Editores. V. 19, 2019. Pág. 295.

> proteger não são os dados em si, mas sim o seu titular, que poderá ser afetado em sua privacidade caso alguns limites não sejam estabelecidos."[25]

Observa-se, portanto, que a LGPD veio no plano infraconstitucional como um norteador para o assunto da proteção de dados pessoais, especificando com detalhes as hipóteses em que referidos dados podem ser legitimamente tratados, e de que forma isso pode ocorrer.

Neste cenário, os empregadores deverão providenciar com a máxima urgência uma readequação de toda a sua rotina, sob pena de sofrerem um isolamento jurídico que acarreta a perda de oportunidades valiosas de investimento financeiro internacional.

A necessidade de adequação surge, ainda, diante das severas penalidades previstas pela legislação atinente à matéria. As multas previstas pela LGPD podem chegar a até 2% do faturamento da empresa fiscalizada, limitado a R$ 50 milhões, além de bloqueio ou eliminação dos dados relacionados a uma infração.

Além de ser uma obrigação legal, a necessidade de adequação por parte das empresas à LGPD vem ainda da evidente tendência de mercado em agregar valor à marca e à empresa em razão da maior transparência e controle dos dados que estão sob seu poder. Dessa forma, reitera-se o risco de um isolamento mercantil das empresas que não dispuserem do nível de proteção de dados adequado.

Não obstante as sanções administrativas, a LGPD dispõe ainda, em artigo 42, que a empresa que não observar o texto legal poderia ser responsabilizada civilmente ao estipular que o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, será obrigado a repará-lo.

2.1 Conceitos básicos, sujeitos e objeto de regulamentação

Como já visto, a LGPD dispõe em seu artigo 1º, *caput*, que a Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. As

[25] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo. Saraiva. 2014. Pág. 32

disposições existentes no texto legal são de interesse nacional e de observância pela União, Estados, Distrito Federal e Municípios.

Conforme aduzido por Lara R. Garcia (2020, p. 16), "A LGPD não tem como escopo os dados das empresas (pessoas jurídicas), mas sim os dados que as empresas têm das pessoas físicas, sejam elas funcionárias, terceiras, clientes, acionistas etc. – ou seja, todo mundo."

A eficácia subjetiva da LGPD abrange todos os sujeitos, seja pessoa natural ou pessoa jurídica de direito público ou privado, que realizem o tratamento de dados pessoais, inclusive nos meios digitais. Para fins do presente trabalho, significa dizer que se aplica tanto a empregados públicos quanto a empregados privados.

Na verdade, aplica-se a LGPD 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, desde que a operação de tratamento seja realizada no território nacional e com objetivo de ofertar ou fornecer bens ou serviços ao mercado consumidor brasileiro ou, ainda se os dados forem coletados no território nacional, assim considerados como aqueles cujo titular nele se encontre no momento da coleta.

Significa dizer que não são levados em consideração o país sede da empresa, o meio de tratamento de dados, a localização dos dados e nem mesmo a nacionalidade de seu titular, bastando apenas que os dados se encontrem em território brasileiro no momento da coleta.

Ainda, para melhor análise e estudo da lei, faz-se necessário conhecer os conceitos básicos trazidos em seu artigo 5º. Assim, para fins da LGPD, considera-se:

> **I - dado pessoal**: informação relacionada a pessoa natural identificada ou identificável;
>
> **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;
>
> **III - dado anonimizado**: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (Redação dada pela Lei nº 13.853, de 2019)

IX - agentes de tratamento: o controlador e o operador;

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

XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas

> competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;
>
> **XVII - relatório de impacto à proteção de dados pessoais**: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;
>
> **XVIII - órgão de pesquisa**: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e (Redação dada pela Lei nº 13.853, de 2019)
>
> **XIX - autoridade nacional**: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. (Redação dada pela Lei nº 13.853, de 2019)

Observa-se que o artigo 5º não traz, por exemplo, o conceito de pseudonimização, encontrado no artigo 13 § 4º da LGPD. A pseudonimização se refere ao tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro[26].

2.2 Fundamentos basilares da lei

Em seu artigo 2º, a LGPS dispõe sete fundamentos que permeiam a disciplina da proteção de dados pessoais e que devem servir de balizadores para dirimir quaisquer questionamentos envolvendo a proteção de dados pessoais. Vejamos:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> II - a autodeterminação informativa;

[26] OHM, Paul. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. UCLA Law Review, Vol. 57, p. 1701, 2010 U of Colorado Law Legal Studies Research Paper No. 9-12. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006 Acesso em: 02 de fevereiro de 2021.

> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Embora todos os sete fundamentos acima listados possuam igual relevância e importância, a autodeterminação informativa não era muito difundida até a edição da LGPD, adquirindo especial destaque a partir da criação da norma.

Inicialmente reconhecido pelo Tribunal Constitucional Alemão durante julgado do caso da Lei do Censo Alemã, esse direito veio para contestar a crença bastante generalizada no sentido de que os dados das pessoas naturais faziam parte do patrimônio da empresa que os coletava. Surgindo como uma solução para vazamentos e diversas utilizações indevidas de dados, a autodeterminação informativa passa a devolver ao titular a decisão acerca da informação e disponibilidade de seus dados.

De fato, o direito à autodeterminação informativa se equipara a um direito fundamental, posto que está diretamente ligado à privacidade e intimidade da pessoa e se traduz na faculdade de o próprio particular determinar e controlar a utilização dos seus dados pessoais[27].

Trata-se do empoderamento do titular na gestão e controle de seus dados[28].

O direito à autodeterminação informativa pode ser mais bem visualizado quando pensamos no exemplo de uma entrega de atestado médico no qual constou a indicação de uma doença (CID). Embora o empregado possua pleno direito de que a informação por ele prestada acerca de seu estado de saúde não seja compartilhada com outras pessoas, o empregador tem não apenas o direito, mas o dever, de realizar a guarda da documentação, inclusive para posteriores fins previdenciários.

O titular dos dados pessoais deve fornecer o seu consentimento de modo claro, expresso e esclarecido, de forma que a empresa possa dar a destinação e tratamento adequados. Nesse sentido leciona Tarcísio Teixeira e Ruth Maria Guerreiro Armelin:

> "Consentimento do titular de dados é a forma mais conhecida de tratamento legal de dados e deve ser livre e o mais consciente possível, ou seja, o titular

[27] CANOTILHO, JJ Gomes. Direito Constitucional e Teoria da Constituição. Coimbra: Almedina, 2003.
[28] Neste sentido, YOSHIDA, Victoria Melo. Autodeterminação informativa, riscos cibernéticos e proteção de dados pessoais: a emergência de um novo compliance. In Revista do curso de direito da Unifacs. Porto Alegre. Paixão Editores. V. 19, 2019. Pág. 295.

> deve ter pleno conhecimento de quais dados estão sendo captados e exatamente para qual fim ele será utilizado, o qual perfaz a inequivocidade do consentimento"[29]

Nesse contexto, imperioso se faz que a empresa esteja preparada para desenvolver rotinas em seus ambientes de trabalho de forma a cumprir o seu dever sem violar o direito de seu trabalhador, através do armazenamento de referidas documentações em setores seguros ou de forma criptografada.

Necessário se faz, ainda, que as pessoas jurídicas de direito privado revejam os seus contratos, especialmente os de trabalho e os termos de uso do consumidor, de forma a constar informações claras e expressas acerca dos tipos de dados que estão serão por elas coletados, por quanto tempo permanecerão armazenados, de que forma se dará esse armazenamento e, ainda, para quais finalidades serão utilizados.

Nesse sentido, as autoras americanas Aleecia M. McDonald e Lorrie Faith Cranor esclarecem que quanto mais complexos forem os textos das políticas de privacidade, mais difícil será que os usuários efetivamente parem para ler e compreender o seu conteúdo, sendo esse um dos principais problemas para melhor compreensão da tutela adequada à proteção de dados[30].

A possibilidade do uso de criptografia, anonimização ou pseudonimização são inclusive cogitados pela própria LGPD, exigindo das empresas (controlador) cada vez mais um esforço combinado com outras áreas, como a tecnologia da informação.

2.3 Hipóteses legais de não aplicabilidade da lei

A LGPD dispõe, em seu artigo 4º, que o seu texto legal não se aplica, entre outras coisas, ao tratamento de dados pessoais realizado por pessoa natural para fins exclusivamente particulares e não econômico. Vejamos:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
> I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

---

[29] TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca. Lei geral de proteção de dados pessoais. Salvador. Juspodivm. 2019. Pág. 43.

[30] MCDONALD, Aleecia M.; CRANOR, Lorrie Faith. Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising. Acesso em: 19 de fevereiro de 2020. Disponível em: https://www.researchgate.net/publication/228237033_Beliefs_and_Behaviors_Internet_Users'_Understanding_of_Behavioral_Advertising

> II - realizado para fins exclusivamente:
> a) jornalístico e artísticos; ou
> b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
> III - realizado para fins exclusivos de:
> a) segurança pública;
> b) defesa nacional;
> c) segurança do Estado; ou
> d) atividades de investigação e repressão de infrações penais; ou
> IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

Observa-se que no âmbito empresarial, portanto, não se verifica margem para afastamento da incidência das obrigações previstas na LGPD, sendo certo que as pessoas jurídicas de direito privado sofrerão fiscalização e cobranças realizadas pela ANPD e pelos próprios titulares dos dados.

Diante da redação contida no inciso I, existe divergência na doutrina acerca da aplicabilidade da LGPD aos empregadores domésticos, tendo em vista que dispõe o artigo 1º da Lei Complementar 150 de 2015 dispõe que empregado doméstico é aquele que presta serviços de forma contínua, subordinada, onerosa e pessoal e de finalidade não lucrativa à pessoa ou à família, no âmbito residencial destas, por mais de 2 (dois) dias por semana.

Nesse aspecto, parece claro que a LGPD, de fato, não é aplicável às relações de trabalho doméstico, por não se vislumbrar qualquer atividade econômica por parte do empregador.

Entretanto, para os doutrinadores que defendem a aplicabilidade da lei nesse tipo de relação trabalhista, é afirmado que empregado doméstico, a depender das atividades desempenhadas na sua função, pode sim realizar tarefas com fins econômicos, e que por isso não entraria na regra de exclusão.

Nessa linha de pensamento é defendido, ainda, que os dados do empregado doméstico são compartilhados com o Poder Público - órgãos previdenciários e fiscais -, não se tratando para fins exclusivamente particulares e, portanto, atrairia a plena aplicação da LGPD.

Tendo em vista que a LGPD ainda conta com apenas alguns meses desde a sua entrada em vigor, os Tribunais Trabalhistas ainda não sedimentaram entendimento sobre a aplicabilidade da lei aos empregadores domésticos. De qualquer forma, caberá à ANPD editar normas complementares a respeito para que seja obtida uma segurança jurídico quando ao assunto em questão.

Observa-se do artigo supratranscrito, mais precisamente nas alíneas *a* e *b* do inciso II, que a LGPD igualmente não se aplica ao tratamento realizado para fins exclusivamente jornalístico e artísticos ou acadêmicos, aplicando-se a esta última hipótese os artigos 7º e 11 da lei.

Também não se aplica a LGPD ao tratamento de dados pessoais provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na lei.

Da mesma forma, não se aplicam os termos da LGPD ao tratamento realizado para fins exclusivos de segurança pública; defesa nacional; segurança do Estado; atividades de investigação e repressão de infrações penais.

2.4 Eficácia espacial da lei

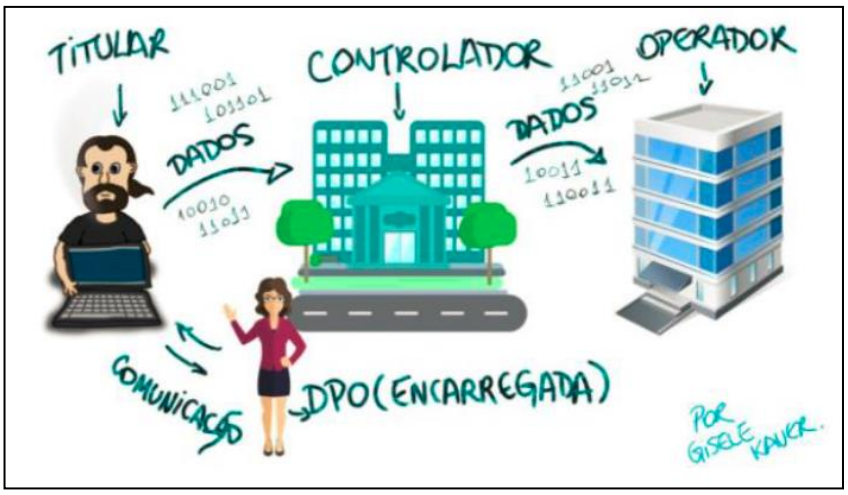
A LGPD se aplica a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

i. a operação de tratamento seja realizada no território nacional, exceto os provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei; ou
ii. a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
iii. os dados pessoais objeto do tratamento tenham sido coletados no território nacional, considerando-se como “coletados no território nacional” os dados pessoais cujo titular nele se encontre no momento da coleta.

2.5 Observâncias a serem feitas pelas empresas para fins de cumprimento

Com o objetivo de atender as exigências feitas pela LGPD, faz-se necessário que as empresas adotem procedimentos a serem observados e seguidos diante das demandas formuladas pelos titulares dos dados, surgindo assim a obrigação de disponibilização de determinadas atividades que serão exercidas pelos sujeitos envolvidos nos tratamentos dos dados pessoais (controlador, operador e encarregado).

Inicialmente, de forma a melhor entender os sujeitos envolvidos nos tratamentos dos dados pessoais, utilizamos-nos da brilhante ilustração realizada por Gisele Kauer[31]:



O **controlador** é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, conforme dispõe o artigo 5º, inciso VI, da LGPD.

Na GDPR, o controlador é descrito como "a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais" (artigo 4º, item 7, da GDPR).

Pode-se afirmar que o controlador é, portanto, as próprias empresas que recebem os dados dos titulares, sejam eles consumidores e/ou empregados, e que detém o domínio dos fatos em se tratando das operações de tratamento. É ele quem recebe os dados e fica responsável por decidir acerca do fluxo de obtenção, tratamento, utilização e descarte.

---

[31] Disponível em: https://www.infranewstelecom.com.br/controlador-operador-encarregado-quem-e-quem-na-lgpd/

Essa definição prevista na GDPR pode ser dividida em três grandes grupos constituintes. Em primeiro lugar, se tratando do aspecto subjetivo, o controlador é a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo. Em segundo, acerca da possibilidade de controle coletivo, isso é, de realizar o controle dos dados em conjunto com outrem. Em terceiro estão os elementos essenciais que permitem distinguir o responsável pelo tratamento (controlador) de outros intervenientes.

O controlador é identificado na prática, portanto, por aquele que de fato determina o modo pelo qual os dados serão tratados, por ser ele quem tem o poder decisório sobre a realização da operação de tratamento.

Para fins do presente trabalho e análise da LGPD sob a ótica das relações trabalhistas o controlador é, em regra, o empregador, por ser ele o responsável pelas operações de tratamento dos dados pessoais de seus empregados. Entretanto, é necessário observar que na hipótese de compartilhamento de dados pelo empregador com empresa terceirizada para realização da gestão da folha de pagamento, por exemplo, esta também será considerada como controlador para fins de aplicação da LGPD.

O **operador**, por sua vez, é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, conforme dispõe o artigo 5º, inciso VII, da LGPD. O artigo 39 da LGPD dispõe ainda que o operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

A GDPR o nomeia de “subcontratante”, e o define como sendo “uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes” (artigo 4º, item 8, da GDPR).

É, portanto, o responsável pelo efetivo tratamento dos dados pessoais na prática, podendo se revelar na figura de um funcionário da empresa receptora dos dados/controlador, caso a empresa opte por tratar os dados no seio da sua organização, ou na figura de um autônomo ou pessoa jurídica que realizará o tratamento dos dados pessoais em nome do controlador.

No geral o operador é alguém ou alguma empresa com experiência na área de tecnologia da informação e tratamento de dados, sendo que a sua existência depende de decisão tomada pelo responsável pelo tratamento do dado – o controlador.

Entretanto, caso o controlador não terceirize as atividades de operação e opte por designar um empregado para o exercício das tarefas de processamento de dados, surge a

dúvida, ainda não dirimida, se o empregado será visto, sob o ponto de vista jurídico, como operador ou se simplesmente será um *longa manus* do controlador.

Em atenção ao artigo 39 da LGPD, que dispõe que o operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, pode se afirmar que, caso o operador não observe às orientações passadas pelo controlador e sim proceda de acordo com suas próprias instruções, será considerado um controlador por equiparação.

Ao disciplinar acerca da responsabilidade civil e do ressarcimento de danos em razão de conduta praticada durante o exercício de atividade de tratamento de dados pessoais, a LGPD prevê, em seu artigo 42, § 1º, inciso I, que o operador responde solidariamente pelos danos causados pelo tratamento quando: (i) descumprir as obrigações da legislação de proteção de dados ou (ii) não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador.

Dessa forma, o operador por equiparação restará caracterizado tão somente na hipótese na qual não forem seguidas as instruções lícitas do controlador, sendo que também será responsabilizado de forma solidária do operador nos casos em que descumprir as obrigações da legislação de proteção de dados[32].

Nesse sentido explana FARIAS, Cristiano Chaves de; BRAGA NETTO, Felipe; ROSENVALD, Nelson. Manual de direito civil: volume único. Salvador. Ed, Juspodivm, 2017, Pág. 1288:

> Se a função do empregado, de algum modo, ensejou o dano, a responsabilidade do empregador não será afastada. O empregado que tem acesso, em razão da função, a informações privilegiadas, e as usa fora do serviço para causar danos, empenha responsabilidade solidária do empregador.

Entretanto, nessa última hipótese, o operador será responsabilizado na qualidade de operador e não na de controlador por equiparação, sendo que na prática a consequência é a mesma.

Ocorrido o dano, surge o dever do empregador/controlador a indenizá-lo na medida de suas condutas, culpabilidade e extensão do dano.[33]

---

[32] FARIAS, Cristiano Chaves de; BRAGA NETTO, Felipe; ROSENVALD, Nelson. Manual de direito civil: volume único. Salvador. Ed, Juspodivm, 2017, Pág. 1288.

[33] TARTUCE, Flávio. Direito das Obrigações e Responsabilidade Civil. 9. ed. São Paulo: Método, 2014. Pág. 409.

Por fim, o **encarregado**, também conhecido pela GDPR como "DPO" (Data Protection Officer), é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD, conforme dispõe o artigo 5º, inciso VIII, da LGPD.

O encarregado não é considerado um agente de tratamento, já que apenas o são o controlador e o operador, conforme dispõe o artigo 5º, inciso IX, da LGPD. Ele é, no entanto, a pessoa responsável por fazer toda a interface entre os consumidores, os empregados e os demais titulares de dados pessoais com o controlador e operador, fazendo com que o fluxo de procedimentos a serem adotados tramite corretamente e atenda as demandas exigidas pela LGPD.

Conforme dispõe o artigo 41 da LGPD, todo controlador é obrigado a indicar um encarregado pelo tratamento de dados pessoais. Contudo, o parágrafo terceiro do mesmo dispositivo prevê que a ANPD poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação.

O parágrafo primeiro de referido artigo dispõe ser obrigatória a divulgação pública da identidade e das informações de contato do encarregado, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador (artigo 41, § 1º, da LGPD).

Isso porque, entre as atividades do encarregado está a de aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências, o que torna imprescindível que sua identidade e as suas informações de contato sejam divulgadas publicamente, de forma clara e objetiva.

Além de aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências, as atividades desenvolvidas pelo encarregado envolvem receber comunicações da autoridade nacional e adotar providências; orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais e executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares, conforme prevê o § 2º do artigo 41 da LGPD, através de um rol exemplificativo.

O artigo 39 da GDPR também estabelece algumas funções do encarregado, como, exemplificativamente: informar e aconselhar o responsável pelo tratamento (controlador) ou o operador, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações nos termos do regulamento e de outras disposições de proteção de dados da União ou dos

Estados-Membros; controlar a conformidade com o regulamento, com outras disposições de proteção de dados da União ou dos Estados-Membros e com as políticas do responsável pelo tratamento ou do operador relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes; prestar aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controlar a sua realização; cooperar com a autoridade de controle; ser ponto de contato para a autoridade de controle sobre questões relacionadas com o tratamento.

De uma breve leitura da LGPD observa-se que esta foi omissa em alguns pontos relacionados ao encarregado.

Questiona-se, por exemplo, se é necessário que o encarregado possua um conhecimento jurídico-regulatório para que possa atuar como tal. A GDPR, por exemplo, estabelece que o encarregado deverá ser assim designado com base nas suas qualidades profissionais e, ainda, com base nos seus conhecimentos especializados no assunto. Entretanto, a LGPD nada fala a respeito.

Na realidade, o dispositivo que previa expressamente que o encarregado deveria ser detentor de conhecimento jurídico-regulatório foi vetado pelo Presidente da República, que assim afirmou na Mensagem nº 288 de 8 de julho de 2019:

> "O Ministério da Economia e a Controladoria-Geral da União, solicitaram ainda, veto ao dispositivo a seguir transcrito:
> § 4º do art. 41 da Lei nº 13.709, de 14 de agosto de 2018, alterado pelo art. 2º do projeto de lei de conversão
> "§ 4º Com relação ao encarregado, o qual deverá ser detentor de conhecimento jurídico-regulatório e ser apto a prestar serviços especializados em proteção de dados, além do disposto neste artigo, a autoridade regulamentará:
> I - os casos em que o operador deverá indicar encarregado;
> II - a indicação de um único encarregado, desde que facilitado o seu acesso, por empresas ou entidades de um mesmo grupo econômico;
> III - a garantia da autonomia técnica e profissional no exercício do cargo."
> **Razão do veto**
> **'A propositura legislativa, ao dispor que o encarregado seja detentor de conhecimento jurídico regulatório, contraria o interesse público, na medida em que se constitui em uma exigência com rigor excessivo que se reflete na interferência desnecessária por parte do Estado na discricionariedade para a seleção dos quadros do setor produtivo, bem como ofende direito fundamental, previsto no art. 5º, XIII da Constituição da República, por restringir o livre exercício profissional a ponto de atingir seu núcleo essencial.'**"

Portanto, observa-se não ser obrigatório que o encarregado possua conhecimento jurídico-regulatório. Entretanto, é recomendado que, na prática, seja escolhido um profissional detentor dessas características, pelo único motivo de que a natureza das atribuições de um encarregado torna necessário esse conhecimento.

A LGPD também é omissa a respeito da possibilidade de se terceirizar as atividades do encarregado.

Embora na redação inicial da LGPD houvesse a previsão de que o encarregado deveria obrigatoriamente ser pessoa natural, essa determinação foi suprimida, passando a prever que o encarregado seja pessoa jurídica, contratada por meio de terceirização de serviços, tal como já era permitido no artigo 37, inciso VI da GDPR.

Dentre a transferência da execução de quaisquer atividades de uma empresa, conforme expressamente autorizado pela Lei nº 6.019/1974, com redação dada pela Lei nº 13.467/2017[34], está a de processamento de dados ou a das atribuições do encarregado. Deve se ter cautela, no entanto, quanto à responsabilidade de se terceirizar referida atividade, já que poderá aumentar as chances de um eventual vazamento de dados.

Com relação à possibilidade de o encarregado exercer outras atividades na empresa, embora a LGPD também seja omissa, podemos usar a GDPR como direito comparado, por ser uma das fontes do direito do trabalho, conforme artigo 8º da CLT.

E, sobre o assunto, o artigo 38, item 6, da GDPR prevê que o encarregado pode sim exercer outras atividades e funções na empresa, desde que não resultem em um conflito de interesses com as tarefas desempenhadas como encarregado.

Um exemplo de conflito de interesses seria o caso das diretorias que não sejam exclusivas para a proteção de dados, recursos humanos, marketing, inovação, comercial/vendas etc.[35].

Com relação à possiblidade de o encarregado poder ou não ser penalizado durante o regular desempenho de suas funções, novamente devemos recorrer à GDPR para orientação. Sobre o assunto, a norma europeia dispõe que o controlador e operador devem garantir autonomia técnico-funcional ao encarregado, ainda que ele seja empregado da empresa.

---

[34] Art. 4o-A. Considera-se prestação de serviços a terceiros a transferência feita pela contratante da execução de quaisquer de suas atividades, inclusive sua atividade principal, à pessoa jurídica de direito privado prestadora de serviços que possua capacidade econômica compatível com a sua execução. (Redação dada pela Lei nº 13.467, de 2017)

[35] LEITÃO, Nairane Farias Rabelo. Decisão belga sobre proteção de dados pode ter reflexo no Brasil. Disponível em: <https://www.conjur.com.br/2020-jun-02/nairane-leitao-protecao-dados-belgica-brasil> Acesso em 06/03/2021.

Essa autonomia não deve ser vista como incompatível com a subordinação jurídica típica das relações de trabalho subordinado, de forma que, embora empregado, o encarregado não deverá receber instruções relativamente ao exercício das suas funções, tampouco poderá ser penalizado pelo controlador ou pelo operador pelo mero fato de exercer regularmente as suas funções.

O encarregado, portanto, será responsável pelo primeiro contato do titular dos dados ou da ANPD e demais órgão de controle, bem como pela devida e correspondente resposta nos termos exigidos pela nova legislação.

Os três sujeitos mencionados (Controlador, Operador e Encarregado) formam um grupo interdisciplinar de modo a garantir aos titulares dos dados e à ANPD transparência nas respostas sobre a forma de utilização dos dados, meios de acesso, pedidos de retificação/atualização, tempo de uso e respectivas finalidades da coleta.

São responsáveis, ainda, por gerar um relatório de impacto à proteção de dados, o qual representa o princípio da responsabilização e prestação de contas. De fato, não é suficiente que o controlador cumpra a lei, sendo absolutamente necessário que, a todo tempo, haja a demonstração desse efetivo cumprimento.

Nesse mencionado relatório, deverão se demonstrados os tratamentos de dados realizados, devendo conter a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação essas medidas. Trata-se de uma forma eficaz de demonstrar a conformidade por parte do controlador, conforme leciona Fabrício da Mota Alves[36].

Ao controlador e operador cabe, ainda, a manutenção do registro das operações de tratamento de dados pessoais, diante da necessidade de prestar contas.

Assim, pontuados os conceitos básicos, os principais sujeitos mencionados pela LGPD e as observações a serem feitas pelas empresas para o correto cumprimento da lei, faz-se pertinente analisar questões práticas que ocorrem ou podem vir a ocorrer em uma relação trabalhista envolvendo o tratamento de dados, bem como de que forma se dará a aplicação da LGPD nesses casos.

3. Situações práticas no direito do trabalho envolvendo o tratamento de dados

[36] ALVES, Fabrício da Mota. Avaliação de impacto sobre a proteção de dados. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Ópice, Comentários ao GDPR. São Paulo. Thomson Reuters. 2018. Pág. 186.

As hipóteses que autorizam o tratamento de dados pessoais são previstas pelo artigo 7º da LGPD, enquanto aquelas que autorizam o tratamento de dados pessoais **sensíveis** são estipuladas pelo artigo 11. Vejamos:

As hipóteses nas quais o tratamento de dados pessoais é autorizado	As hipóteses nas quais o tratamento de dados pessoais **sensíveis** é autorizado
Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: 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) ;	Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; e) proteção da vida ou da incolumidade física do titular ou de terceiro;

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro; 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.	f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Da tabela elaborada e acima colacionada é possível observar que a grande diferença entre as bases de tratamento dos dados pessoais e dos dados pessoais sensíveis é que o interesse legítimo do controlador ou de terceiro é hipótese autorizadora para tratamento apenas dos primeiros, conforme inciso IX do artigo 7º.

Ainda, mencionando o exercício regular de direitos, a LGPD esclarece que estes serviriam como justificativa de ados pessoais não sensíveis tão somente diante de processos judiciais, administrativos e arbitrais, enquanto que, para o tratamento de dados pessoais sensíveis, o exercício regular de direitos não está restrito a qualquer tipo de processo.

Cabe ao controlador, figura já estudada no presente trabalho, identificar cautelosamente as bases legais autorizadoras de cada tratamento. Havendo mais de uma hipótese, recomenda-se fortemente a escolha de forma mais conservadora possível, tendo em vista que os princípios da LGPD apontam para um tratamento adequado, limitado e restrito à finalidade legitimadora específica. Conforme leciona Marcelo Novelino, os princípios, diferentemente das regras, devem ser aplicados de forma mitigada quando verificada algum tipo de contraposição[37].

Trazendo a questão para o cerne das relações trabalhistas, as hipóteses previstas na LGPD que servirão como autorizadoras dos tratamentos mais comuns de dados pessoais são: (i) cumprimento de obrigação legal ou regulatória (artigo 7º, II) ALCASSA;

[37] NOVELINO, Marcelo. Direito constitucional. 2. ed. São Paulo: Método, 2008. p. 65-66.

CASTELANI, 2020); (ii) execução de contrato ou de procedimentos preliminares relacionados ao contrato (artigo 7º, V) e (iii) exercício regular de direitos em processo judicial, administrativo ou arbitral (artigo 7º, VI).

Embora os procedimentos que envolvem a fase pré-contratual de um empregado legitimem o acesso a informações sobre o candidato – até de forma a permitir que o empregador faça melhor escolha -, é recomendado muita cautela no que tange às informações que serão exigidas, devendo a empresa se ater estritamente às informações necessárias para o regular exercício da função para a qual a vaga está aberta.

Sempre que possível a empresa deve evitar, portanto, perguntas relacionadas ao gênero, estado civil, existência de filhos, pretensão de contrair matrimônio, religião, doenças prévias, patrimônio genético, antecedentes criminais e investigação de vida financeira.

Campos para preenchimento de indicação de contatos de referência ainda são comuns atualmente, embora a LGPD se manifeste absolutamente contra essa situação.

Em se tratando da fase contratual, diversos dados do empregado serão armazenados pela empresa, como salário, dados relacionados à jornada de trabalho, descontos, faltas e respectivos motivos, situações conjugais e familiares que posam ter reflexos em pensão por exemplo, acidentes, doenças etc.

No período pós-contratual, da mesma forma, existem diversos dados que se revelam necessários para fins de formalização da rescisão contratual, incluindo exame médico demissional.

3.1 *Background checks* - Análise de antecedentes do empregado

A análise dos antecedentes de um empregado, também chamado de *background checks*, é o processo de checagem dos antecedentes do trabalhador ou candidato com o objetivo de verificar a existência de conformidade com a cultura empresarial.

Esses *background checks* incluem a confirmação do histórico de emprego, através do contato com ex-empregadores; autenticação de credenciais educacionais (diplomas e certificações); análise de perfil do candidato ou empregado em redes sociais; verificação de relatórios de crédito e, ainda, pesquisa de antecedentes criminais.

De forma a tentar minimizar os riscos decorrentes do tratamento de dados obtidos nas análises de antecedentes, recomenda-se que o processo de triagem realizado por uma

empresa seja padrão para todos os seus candidatos, retirando a discricionariedade e inserindo a objetividade nos processos seletivos.

Esse processo de triagem e análise de antecedentes está intrinsecamente relacionado com questões de segurança, conformidade legal, responsabilidade e ajuste da empresa. Dessa forma, deve-se criar ambientes seguros para os seus trabalhadores.

Com relação especificamente à realização de consulta de restrições de crédito, a jurisprudência Colendo Tribunal Superior do Trabalho ("C. TST") se posiciona no sentido de que a sua realização por parte do empregador iria contra à Constituição Federal por força da sua proibição de discriminação no âmbito da relação de trabalho (artigo 7º, XXXI), seguindo os parâmetros estabelecidos pela Convenção 111 da OIT.

Deve-se ter em mente, ainda, que os que órgãos de proteção ao crédito não devem ser utilizados para fins de relação de trabalho, posto que destinados a proteger o crédito e não para inviabilizar o emprego.

A exigência de certidão de antecedentes criminais, por sua vez, já foi expressamente trtada por decisão vinculante do C. TST, em acórdão publicado em 22/09/2017, no julgamento do Recurso Repetitivo (RR) 243000-58.2013.5.13.0023, com a fixação da tese jurídica prevalecente no sentido de que a exigência de certidões de antecedentes criminais somente se justifica em casos excepcionais, em virtude da existência de lei, natureza do ofício ou elevado grau de fidúcia.

Na realidade, a própria tese jurídica acima mencionada elenca as atividades em relação às quais é legítima a exigência de certidão de antecedentes criminais, aduzindo que a referida exigência se revela legítima e não caracteriza lesão moral quando amparada em expressa previsão legal ou justificar-se em razão da natureza do ofício ou do grau especial de fidúcia exigido, a exemplo de empregados domésticos, cuidadores de menores, idosos ou deficientes (em creches, asilos ou intuições afins), motoristas rodoviários de carga, empregados que laboram no setor da agroindústria no manejo de ferramentas de trabalho perfurocortantes, bancários e afins, trabalhadores que atuam com substâncias tóxicas, entorpecentes e armas, trabalhadores que atuam com informações sigilosas.

3.2 Utilização de dados biométricos

A LGPD esclareceu de maneira expressa em seu artigo 5º, inciso II, que o dado biométrico deve ser considerado como um dado pessoal "sensível", o que levantou o debate

sobre sua utilização pelos empregadores, os quais o utilizam muito para fins de registro de jornada de seus trabalhadores.

De fato, a necessidade de se registrar a jornada de trabalho do empregado é prevista na própria CLT, a qual, em seu artigo 74, permite que o controle seja realizado por meio manual, eletrônico ou mecânico. A Portaria 1510 de 2009, editada pelo Ministério do Trabalho, também autorizou o ponto biométrico.

Sobre o assunto e analisando o enquadramento de dado sensível trazido pela LGPD, embora seja possível defender que existem outros tipos de controle de jornada que podem ser utilizados pelo empregador, o dado biométrico tem se revelado há anos como um método extremamente eficaz e confiável que evita – ou ao menos diminui – alegações de desvirtuamento da jornada pela existência de controles de ponto paralelos.

O controle de jornada realizado através do controle biométrico, portanto, está assegurado pelo cumprimento de obrigação legal por parte do controlador, conforme prevê o artigo 11, inciso II, alínea *a*, da LGPD, não necessitando da autorização expressa do empregado.

A utilização do controle biométrico também está autorizada, sem necessidade do consentimento do empregado, caso seja utilizado para controle de acesso e segurança na empresa, incidindo nesta hipótese a alínea *g* do inciso II do artigo 11 da LGPD.

No caso concreto, entretanto, será observada sempre a intenção do empregador, devendo restar inequívoco que os dados obtidos estão sendo utilizados com a finalidade estrita para os quais foram colhidos.

Essa necessidade de estar sempre demonstrado que o tratamento dos dados se dê com uma finalidade estritamente necessária, adequada e proporcional, além da aplicação da forma sempre menos intrusiva possível, leva para os empregadores o ônus de comprovar que estão tomando todas as medidas adequadas com o objetivo de equilibrar a intenção de se chegar a uma finalidade e o respeito à liberdade dos empregados e titulares dos dados fornecidos.

3.3 Fiscalização das redes sociais do empregado

Em uma situação na qual o empregador esteja fiscalizando as páginas de redes sociais de um ex empregado com o intuito de verificar, exemplificativamente, se as cláusulas de não concorrência ou de confidencialidade constantes em seu extinto contrato de trabalho

estão sendo cumpridas, é possível afirmar que age a empresa de forma legítima, já que este tratamento de dados está, em tese, balizado na necessidade de se proteger os legítimos interesses dos negócios.

Em parecer emitido sobre o tema, o órgão consultivo europeu independente em matéria de proteção de dados e privacidade ("GT29") entendeu que, sendo o monitoramento restrito aos ex-empregados (no exemplo citado) e com o fito de observar a conformidade de suas atitudes com cláusulas todavia válidas – esse objeto deve ser efetivamente demonstrado, essa fiscalização seria válida (ponto 5.2 do Parecer 2/2017 do GT29).

Importante ressaltar, neste ponto, que, em que pese seja sempre importante obter, quando possível, a autorização expressa por parte do empregado, não há como negar que é improvável que esses consentimentos sejam fornecidos de forma espontânea, de forma, que, para a própria diminuição de riscos para o empregador, seria importante sempre se resguardar obtendo um fundamento legal para os atos praticados que não fosse apenas no consentimento dos trabalhadores, conforme será mais bem analisado no tópico seguinte.

3.4 *Imbalance of power*. O consentimento dado pelo empregado

Embora o consentimento concedido pelo titular dos dados seja uma hipótese legitimadora para tratamento de dados pessoais (sensíveis ou não), conforme prevê o artigo 7º, inciso I, da LGPD, nas relações de trabalho a utilização deste consentimento traz consigo algumas cautelas a serem observadas.

A problemática apresentada se revela desde a análise o próprio conceito de consentimento previsto na LGPD. Em seu artigo 5º, inciso XII, a lei dispõe que o consentimento deve ser entendido como a *manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada*.

A expressão "livre" trazida pela LGPD pressupõe verdadeira opção do titular dos dados, o que levanta dúvidas, sobre a possibilidade de sua ocorrência no seio de uma relação de trabalho, a qual é marcada pelo desequilíbrio poder entre as partes.

Pautar e embasar um tratamento de dados no consentimento fornecido "livremente" por um empregado gerará, sem sombra de dúvidas, alegações de que essa escolha não teria se dado de forma tão livre assim, e que, ao contrário, o empregado não teria tido legítima escolha ao concordar com o uso de seus dados.

A GDPR, quando criada, não se omitiu a referida hipótese, tendo estipulado em seu artigo 43 que "a fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto ("imbalance of power") entre o titular dos dados e o responsável pelo seu tratamento".

Embora essa problemática possa ser diluída nos casos em que o empregado se revele hiperssuficiente, nos termos do parágrafo único do artigo 444 da CLT, nos demais casos a empresa estará exposta aos riscos de um questionamento inclusive judicial.

É neste cenário que se verifica que é mais recomendável que a empresa, ao tratar de dados pessoais de seus empregados, evite utilizar o consentimento como base legal autorizadora para tanto. Entretanto, caso não seja possível enquadrar a situação em alguma das ouras hipóteses permissivas, deve ser observado o que dispõe o artigo 8º, § 1º da LGPD:

> Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.
> § 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.

Como se observa, o consentimento deve ser fornecido por escrito ou por outro meio que demonstra a manifestação de vontade do titular. Caso seja por escrito, a cláusula do consentimento deve estar destacada das demais.

Em algumas hipóteses específicas, como consentimento para utilização de dados para fins de realização de rankings de produtividade entre funcionários da empresa, seria interessante que fosse celebrado um documento de autorização em apartado do contrato de trabalho para que se tente evitar futuros questionamentos.

Também deve se observar que o consentimento obtido do empregado pela empresa para tratamento de seus dados não pode ser genérico, nos termos do § 4º do artigo 8º da LGPD, sob pena de ser considerado inválido. Ao contrário, deve ser fornecido ao empregado todas as informações relativas a esse tratamento, inclusive a finalidade específica para a qual será utilizado.

A autorização expressa e consentida para tratamento dos dados do empregado não autoriza o compartilhamento de seus dados com outros controladores (empresas terceirizadas, planos de saúde etc.) sem um novo e específico consentimento, nos termos do artigo 7º, § 5º da LGPD.

Caso os dados que a empresa queira realizar o tratamento sejam tornados manifestamente públicos pelo titular, dispõe o artigo 7º, § 4º que o consentimento será dispensado, o que não significa que poderão ser utilizados para finalidades diversas daquela inicialmente estipulada.

Importante observar que o Compliance se revela como uma ótima ferramenta para auxiliar a empresa a realizar o tratamento adequado de dados. Nesse sentido explica o Procurador do Trabalho, Henrique Correia (2018, p. 2) que:

> Compliance é um termo originário de língua inglesa derivada do verbo to comply que significa "agir conforme uma regra, uma instrução". Compreende uma prática empresarial que consiste na criação de um sistema de controle e fiscalização interno na empresa para reduzir os riscos à imagem do negócio por meio do correto cumprimento das normas aplicáveis à instituição. Assegura-se, portanto, a transparência da empresa em relação à sociedade.

Por fim, deve a empresa observar que o empregado pode revogar eventual consentimento concedido a qualquer momento, nos termos § 5º do artigo 8º da LGPD, o que ratifica os riscos em basear o tratamento de dados pessoais no consentimento concedido pelo empregado.

4. Sanções estabelecidas pela LGPD

Como visto, a LGPD prevê diversos direitos aos titulares de dados pessoais, bem como uma série de obrigações para as empresas (controlador). A observância das regras contidas na lei em vigor desde setembro de 2020 é obrigatória, sendo que no caso de descumprimento a empresa empregadora será responsabilizada pela reparação dos danos eventualmente causados, sem prejuízo de responder por outras sanções administrativas aplicadas pela ANPD.

ANPD, muito citada no presente trabalho, foi criada pela Lei Federal nº 13.853/2019 (artigo 55-A) para atuar como órgão responsável pelo zelo, implementação e fiscalização do cumprimento da LGPD.

O Governo Federal, logo em seguida à vigência da LGPD, publicou, em 27 de setembro de 2020, o Decreto 10.474/20, que instituiu a estrutura regimental do órgão e o quadro demonstrativo dos cargos em comissão e das funções de confiança, porém, ainda sem

a formação e nomeação dos seus membros do conselho diretor, o que só veio ocorrer em 06 de novembro do mesmo ano.

A ANPD é órgão da administração pública responsável por zelar e executar os dispositivos da LGPD, bem como fiscalizar o seu cumprimento em organizações públicas e privadas e aplicar sanções em casos de descumprimento da legislação em todo o território nacional, conforme dispõe o artigo 5º, XVIX, da LGPD.

De fato, é possível afirmar que, sem a atuação efetiva de uma Autoridade Nacional Reguladora, provavelmente a LGPD não produziria efeitos concretos na prática, tendo em vista que suas diretrizes provavelmente não seriam implementadas de forma efetiva sem a atuação de um órgão responsável pela promoção, orientação e fiscalização de sua aplicação.

A relevância da ANPD é tanta que o texto legal aprovado lhe faz menção em pelo menos 40 (quarenta) disposições, citando-a para as mais diversas finalidades.

Dentre as atribuições da ANPD, destacam-se as seguintes: (a) zelar pela proteção de dados pessoais, dos segredos comerciais e industriais; (b) fiscalizar e aplicar sanções no caso de descumprimento da LGPD; (c) apreciar petições de indivíduos contra controladores de dados; (d) solicitar relatórios de impacto ao controlador de dados pessoais; (e) determinar as hipóteses de dispensa de nomeação do Encarregado (“DPO”); (f) dispor sobre padrões técnicos mínimos de segurança aptas a proteger acessos não autorizados; (g) receber as comunicações de incidente envolvendo dados pessoais; (h) promover ações de cooperação com autoridades de proteção de dados de outros países; (e) editar regulamentos e procedimentos sobre a proteção de dados pessoais e privacidade; dentre outras.

A ANPD segue o formato europeu de proteção de dados e tem como inspiração o formato das Autoridades Europeias, em especial, a ICO Inglesa; o CNIL, da França; o Garante Privacy, Autoridade de Proteção de Dados Italiana; e a OPC do Canadá. Mantendo um formato de horizontalidade, a ANPD é de aplicabilidade geral e ampla, podendo ser aplicada a qualquer organização – pública e privada – que realiza tratamento de dados pessoais.

Isto quer dizer que a LGPD brasileira é uma Lei de dados que se aplica a todos, desde uma empresa de pequeno porte como uma academia de ginástica, até uma grande empresa de tecnologia que trabalha, por exemplo, só com análises de dados.

Não apenas a ANPD, mas os próprios titulares dos dados (os empregados, por exemplo) e auditores fiscais do trabalho poderão e deverão fiscalizar a aplicação da LGPD

exercendo seu extenso rol de direitos e podendo levar o caso ao Poder Judiciário e ao Ministério Público do Trabalho, quando necessário, para obter a tutela em relação aos seus dados.

Assim, demonstrada que a empresa coletora dos dados – no presente trabalho exemplificada pela empresa empregadora - não observou os ditames legais previstos na LGPD, haverá a implicação das sanções previstas no texto legal.

Dentre as sanções administrativas previstas pela LGPD destacam-se as seguintes punições, aplicáveis pela ANPD:

> I - Advertência, com indicação de prazo para adoção de medidas corretivas;
> II - Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III - Multa diária, observado o limite total a que se refere o inciso II;
> IV – Publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V - Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI - Eliminação dos dados pessoais a que se refere a infração;
> VII - Suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 06 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
> VIII - Suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
> IX - Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

É possível observar que as sanções previstas na lei podem inclusive colocar em cheque a própria continuidade da atividade empresarial, na medida em que existe a possibilidade de aplicação de multa de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração e até mesmo bloqueio, suspensão e proibição de tratamento de dados de modo parcial ou total.

As sanções elencadas na lei serão aplicadas, por óbvio, após procedimento administrativo que possibilidade o exercício do contraditório e ampla defesa, de acordo com as peculiaridades do caso concreto.

Observa-se, portanto, que, embora os titulares dos dados também possam ativamente combater eventuais irregularidades observadas, a ANPD tem um papel fundamental não apenas na aplicação de futuras sanções ou na edição de parâmetros de aplicação da LGPD, mas principalmente ao exercer a sua função educacional, de conscientização em relação ao zelo e guarda dos dados pessoais dos cidadãos.

Por esse motivo e considerando que apenas meses se passaram desde a entrada em vigor da LGPD, é extremamente importante acompanharmos os planos e a agenda de atuação da ANPD. No dia 27 de janeiro, a ANPD divulgou – por meio da Portaria nº 11/2021 – sua agenda regulatória até o segundo semestre de 2022:

AGENDA REGULATÓRIA DA ANPD		
1º Semestre de 2021	**1º Semestre de 2022**	**2º Semestre de 2022**
Regimento Interno da ANPD	Direitos dos titulares de dados pessoais	Hipóteses legais de tratamento de dados pessoais
Planejamento Estratégico da ANPD	DPO ou Encarregado de Proteção de Dados	
Estabelecimento de normativos para aplicação das sanções administrativas	Transferência Internacional de Dados Pessoais	
Comunicação de incidentes e especificação do prazo de notificação		
Relatório de impacto à proteção de Dados Pessoais		
Proteção de dados e da privacidade para pequenas e médias empresas, startups e pessoas físicas que tratam de dados pessoais com fins econômicos		

Revela-se um desafio à ANPD para aplicar multas por descumprimento da LGPD o fato de que não existe ainda um regramento específico para o processo administrativo

sancionador, ainda estando pendente que a ANPD elabore regulamento próprio sobre sanções administrativas a infrações, nos termos do artigo 53, *caput*, da LGPD.

Além da multa mencionada, resguarda-se ainda a possibilidade de a empresa ser condenada à indenizar o empregado por danos materiais decorrentes do mesmo ato lesivo, observando-se os critérios balizadores entabulados no artigo 223-G, para a fixação do dano extrapatrimonial[38].

[38] DELGADO, Maurício Godinho; DELGADO, Gabriela Neves. A reforma trabalhista no Brasil com os comentários à lei n. 13.467/2017. São Paulo. LTr. 2017. Pág. 146

CONCLUSÃO

O objetivo geral deste trabalho foi fazer uma análise dos termos da Lei Geral de Proteção de Dados (“LGPD”), considerando o cenário que envolveu a sua criação e os impactos que a lei causa nas relações laborais no que diz respeito à privacidade e à proteção de dado pessoais.

O primeiro capítulo examinou a temàtica da proteção de dados, em seu aspecto histórico, desde os fatores que conduziram a criação deste novo direito, perpassando pela sua regulamentação e culminando na edição da LGPD.

No segundo capítulo, abordou-se, propriamente, a Lei Geral de Proteção de Dados Pessoais no que se refere às relações trabalhistas, esmiuçando os conceitos básicos, os sujeitos e objetos da regulamentação que serviram de alicerce para a criação da lei. Neste ponto do estudo, levantou-se as hipóteses legais de não aplicabilidade da lei, sua eficácia espacial, bem como os procedimentos a serem obervados pelas empresas para o fiel cumprimento da norma.

Na sequência, já no terceiro capítulo, foram examinadas situações práticas no direito do trabalho e de que forma a LGDP se aplica nesses contextos. Foi analisado, por exemplo, até que ponto e de que forma poderá o empregador requerer de seu empregado a apresentação de antecedentes criminais (os chamados *background checks*), ou se a utilização de dados biométricos seria permitida pelo texto legal.

Discutiu-se nesse capítulo, ainda, a necessidade de os empregadores reverem os contratos de trabalho celebrados com seus empregados e a pertinência de se confecionar termos de consentimento a serem assinados pelos empregados, redigido com informações claras e objetivas acerca dos dados pessoais que serão tratados pelo empregador e, ainda, para quais motivos será realizado esse tratamento.

A necessidade de adaptação dos formulários de contratação e dos contratos de trabalho em si pela empresa foi analisada como forma a serem cumpridos os objetivos trazidos na LGPD, sendo proibida qualquer alteração da finalidade de uso dos dados coletados sem o total consentimento do titular.

Também é papel do empregador não permitir que os dados pessoais por ele armazenados e tratados ao longo de uma relação laboral sejam utilizados para fins deturpados, ilícitos ou discriminatórios, sob pena de incorrer em sanções administrativas e cíveis,

conforme também tratado no presente trabalho.

Imperioso se faz que os empregadores estejam prontos para aplicar em seus ambientes laborais todas as medidas cabíveis para proteção do extenso rol de direitos dos trabalhadores enquanto titulares dos dados armazenados e tratados, inclusive em momentos pré-contratuais e pós-contratuais.

Como também debatido no terceiro capítulo, não se revela a melhor das estratégias a obtenção de consentimento dos empregados como base única legal para utilização dos dados pessoais armazenados, o que exige muita cautela do empregador na hora de identificar a melhor hipótese autorizadora para cada caso. Isso porque, como bem explicado, as disposições contratuais existentes em eventual termo de consentimento que venham a causar qualquer dano ao empregado podem ser entendidas como nulas, fazendo cair por terra a autorização legal obtida pelo empregador.

Com relação ao ônus da prova, o terceiro capítulo abordou ainda a quem caberia provar que o consentimento obtido se deu em conformidade com o texto legal previsto na LGPD, revelando uma intenção do legislador em adaptar legalmente o procedimento no âmbito probatório tendo em vista a grande relevância do tema referente à utilização de dados pessoais.

Verificou-se que a LGPD, portanto, eleva consideravelmente os deveres dos empregadores, exigindo uma alteração completa de atitude no que tange ao modo de obter, armazenar e tratas os dados pessoais de seus trabalhadores, sendo inclusive necessário, muitas vezes, uma alteração estrutural no operacional da empresa para que as obrigações trazidas pela LGPD sejam de fato observadas. Esses tratamentos de dados, como vito na monografia, será composta pelo Controlador, Operador e Encarregado (DPO).

Tendo em vista que o legislador brasileiro, ao editar a LGPD, não trouxe em seu texto legal nenhum capítulo único e específico para tratar das relações trabalhistas, já se observa desde já que, na análise do caso concreto, será necessário se utilizar do direito comparado, inclusive através da análise da GDPR, que serviu de tanta inspiração para a lei brasileira. Outra forma de se solucionar os problemas que certamente aparecerão em casos concretos, os empregadores deverão se valer das regras gerais da legislação e, ainda, das normas regulamentares editadas pela Autoridade Nacional de Proteção de Dados (“ANPD”) através de resoluções, portarias ou até mesmo orientações.

Foi o que foi visto no quarto capítulo do presente trabalho, no qual foram analisadas as sanções e as responsabilizações civis passíveis de serem aplicadas pela ANPD às empresas que não cumprirem e não respeitarem as obrigações trazidas pela LGPD.

Conclui-se, portanto, que é imperiosa a imediata adequação das condutas dos empregadores às regras trazidas pela LGPD, abrangendo desde a contratação do empregado até a sua rescisão contratual, devendo as empresas estarem mais do que nunca se protegendo com o objetido de evitar qualquer vazamento de dados ou, ainda, a má utilização deles.

Por fim, como debatido em detalhes no quarto capítulo, a ANPD atuará de maneira ostensiva para fiscalizar a correta aplicação da LGPD na prática das empresas e dos empregadores, não medindo esforços, ao que parece, para adoção das sanções administrativas previstas na norma.

Dessa forma, conclui o presente trabalho ser extremamente necessário que, do ponto de vista jurídico, os empregadores, para se adaptarem às regras da LGPD, revisem os termos de uso de seus serviços, bem como políticas de privacidade; revisem os contratos de trabalho e aditivos celebrados com seus empregados, bem como os instrumentos jurídicos relacionados (assistência médica, folha de pagamento, contabilidade etc.); definam quem efetuará as atividades de Operador e Encarregado (DPO); bem como que sejam estabelecidos procedimento com o intuito de controlar o fluxo de dados e ter um acervo probatório para o caso de vir a ser necessário em eventuais fiscalizações.

REFERÊNCIAS

Bibliografias:

AGUIAR, Antonio Carlos. A proteção de dados no contrato de trabalho. Revista Ltr: legislação do trabalho, São Paulo, SP, v. 82, n. 6, p. 655-661, jun. 2018.

ALCASSA, Flávia. O papel da Lei Geral de Proteção de Dados Pessoais. (LGPD) nas relações de trabalho. Revista Síntese: Trabalhista e Previdenciária. Revista Síntese: trabalhista e previdenciária, v. 31, n. 375, p. 58-65, set. 2020.

ALCASSA, Flávia; CASTELANI, Liliana. Lei Geral de Proteção de Dados Pessoais e o Impacto nas Relações de Emprego. Associação Nacional dos Profissionais de Privacidade de Dados. 2020.

ALVES, Fabrício da Mota. Avaliação de impacto sobre a proteção de dados. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Ópice, Comentários ao GDPR. São Paulo. Thomson Reuters. 2018.

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

BEPPLER, Daniela. Internet e informatização: implicações no universo jurídico. In: ROVER, Aires José (Org.). Direito, sociedade e informática: limites e perspectivas da vida digital. Florianópolis: [s.n.], 2000

BITTAR, Carlos Alberto. Os direitos da personalidade. São Paulo. Saraiva. 8 ed. 2015. BOBBIO, N. A era dos Direitos. Tradução de Carlos Nelson Coutinho. Rio de Janeiro: Elsevier, 2004.

BLUM, Renato Opice; MALDONADO, Viviane Nóbrega (Coord.). LGPD comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

CASTELLS, M. A sociedade em rede. A era da informação: economia, sociedade e cultura. Tradução Roneide Venâncio Majer. São Paulo: Paz e Terra, 2016. v.1.

CARLA, R. Direito do trabalho esquematizado. Editora Saraiva, 2017.

CHAVES, Luís Fernando Padro. Responsável pelo tratamento, subcontratante e DPO. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Ópice, Comentários ao GDPR. São Paulo. Thomson Reuters. 2018.

CONI JR, Vicente Vasconcelos. A cibercidadania como consequência de um novo modelo de governança da gestão de políticas púbicas. Florianópolis. Empório do direito. 2019.

DELGADO, Maurício Godinho; DELGADO, Gabriela Neves. A reforma trabalhista no Brasil com os comentários à lei n. 13.467/2017. São Paulo. LTr. 2017.

FARIAS, Cristiano Chaves de; BRAGA NETTO, Felipe; ROSENVALD, Nelson. Manual de direito civil: volume único. Salvador. Ed, Juspodivm, 2017.

GARCIA, L. R. Lei Geral de Proteção de Dados (LGPD): Guia de implantação. Editora Blucher, 2020.

MOREIRA, Teresa Coelho. Compliance digital: direito dos empregados e alcance da responsabilidade da empresa no tratamento de dados. In: TEIXEIRA FILHO, João de Lima (Coord. et. al.). Direito do trabalho no limiar da 4 ª Revolução Industrial: desafios e conformação. Porto Alegre: Lex Magister, 2019.

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

PAMPLONA FILHO, Rodolfo; GAGLIANO, Pablo Stolze. Manual de direito civil: volume único. 1 ed. São Paulo. Saraiva. 2017.

PECK, P. P. Proteção de dados pessoais - comentários à Lei n. 13.709/2018 LGPD. Editora Saraiva, 2018.

SARLET, Ingo Wolfgang. MARINONI, Luiz Guilherme. MITIDIERO, Daniel. Curso de Direito Constitucional. São Paulo: Saraiva, 2018.

SORIANO, Olga Fuentes. La prueba prohibida. Viejos problemas procesles de las nuevas tecnologias. In PRIORI POSADA, Giovanni. Justicia y proceso en el siglo XXI. Desafios y tareas pendientes. Lima. Palestra Editores, 2019.Citar decisão recente.

TARTUCE, Flávio. Direito das Obrigações e Responsabilidade Civil. 9. ed. São Paulo: Método, 2014.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donado (Coord.). A Lei Geral de Proteção de Dados pessoas e suas repercussões no direito brasileiro. 2 ed São Paulo Thomson Reuters Brasil, 2020.

TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca. Lei geral de proteção de dados pessoais. Salvador. Juspodivm. 2019.

YOSHIDA, Victoria Melo. Autodeterminação informativa, riscos cibernéticos e proteção de dados pessoais: a emergência de um novo compliance. In Revista do curso de direito da Unifacs. Porto Alegre. Paixão Editores. V. 19, 2019.

Sítios eletrônicos consultados:

ARAÚJO, Leandro Sampaio Correa de. Impactos da Lei Geral de Proteção de Dados nas relações de trabalho Disponível em: https://www.conjur.com.br/2020-mar-14/leandro- araujo-impactos-lgpd-relacoes-trabalho Acesso em: 08 de dezembro de 2020.

BELLINETTI, L; DE SOUZA, R. Compliance trabalhista: uma análise a partir da função social da propriedade e da responsabilidade socioambiental da empresa. Direitos Fundamentais & Justiça | Belo Horizonte, ano 13, n. 40, p. 221-238, jan. /jun. 2019 Disponível em: http://dfj.emnuvens.com.br/dfj/article/view/741 Acesso em: 10 de dezembro de 2020.

BOLDRIN, Paulo Henrique Martinucci, CORREIA, Henrique. Lei Geral de Proteção de Dados (LGPD) e o Direito do Trabalho. Meu site jurídico. 25 de setembro de 2020. Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2020/09/25/lei-geral-de-protecao-de-dados-lgpd-e-o-direito-trabalho/. Acesso em: 11 de dezembro de 2020.

BRASIL, Lei no 10.406, de 10 de janeiro de 2002. Código Civil. Diário Oficial da União: seção 1, Brasília, DF, ano 139, n. 8, p. 1-74, 11 jan. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm. Acesso em: 12 de dezembro de 2020.

BRASIL. Lei no 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. (Marco Civil da Internet). Disponível em: https://legislacao.presidencia.gov.br/atos/?tipo=LEI&numero=12965&ano=2014&ato=93eUTRE9ENVpWTdb6. Acesso em: 12 de dezembro de 2020.

BRASIL. Lei no 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato20152018/2018/lei/L13709.htm. Acesso em: 12 de dezembro de 2020.

BRASIL, LEI No 14.010, DE 10 DE JUNHO DE 2020. Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19). Brasília. 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14010.htm. Acesso em: 18 de fevereiro de 2021.

CORREIA, Henrique. Compliance e sua aplicação no Direito do Trabalho. Henrique Correia – Direito do Trabalho. Disponível em: http://www.henriquecorreia.com.br/2018/11/blog-post_12.html. Acesso em: 23 de janeiro de 2021.

Directiva 95/46/CE do Parlamento Europeu e do Conselho. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 23 de janeiro de 2021.

INTERNATIONAL LABOUR ORGANIZATION. Protecti on of workers'personal data. An ILO code of practice. Geneva, ILO, 1997. Disponível em: https://www.ilo.org/global/topics/safety-and-health-at-work/normative-instruments/code-of-practice/WCMS_107797/lang--en/index.htm. Acesso em: 10 fevereiro de 2021.

JUNIOR, Carlos Augusto Pinto de Vasconcellos; FERREIRA, Victor Silva. Impacto da lei geral de proteção de dados pessoais nas relações de trabalho: a necessidade de implantação do programa de integridade (Compliance). UERJ Labuta. 21 de março de 2020. Disponível em: https://uerjlabuta.com/2020/03/21/impacto-da-lei-geral-de-protecao-de-dados-pessoais-nas-relacoes-de-trabalho-a-necessidade-de-implantacao-do-programa-de-integridade-Compliance/. Acesso em: 10 de fevereiro de 2021.

Lei de Proteção de Informações Pessoais e Documentos Eletrônicos. Disponível em: https://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html. Acesso em: 10 fevereiro de 2021.

Lei Federal de Proteção de Dados. Disponível em: https://www.gesetze-im-internet.de/bdsg_2018/. Acesso em: 10 de fevereiro de 2021.

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

MIZIARA, Raphael. LGPD: razões de sua existência e impactos nas relações de emprego. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/lgpd-razoes-de-sua-existencia-e-impactos-nas-relacoes-de-emprego-15032020 Acesso em: 22 de março 2021.

MCDONALD, Aleecia M.; CRANOR, Lorrie Faith. Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising. Acesso em: 04 de abril de 2020. Disponível em: https://www.researchgate.net/publication/228237033_Beliefs_and_Behaviors_Internet_Users'_Understanding_of_Behavioral_Advertising.

OLIVIERI, Nicolau. LGPD e sua necessária adequação às relações de trabalho. Disponível em https://www.jota.info/opiniao-e-analise/artigos/lgpd-e-sua-necessaria- adequacao-as-relacoes-de-trabalho-28092019 Acesso em: 13 de janeiro de 2021.

OHM, Paul. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. UCLA Law Review, Vol. 57, p. 1701, 2010 U of Colorado Law Legal Studies Research Paper No. 9-12. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006 Acesso em: 02 de fevereiro de 2021.

REANI, Valéria. O impacto da lei de proteção de dados brasileira nas relações de trabalho. Disponível em: https://www.conjur.com.br/2018-set-21/valeria-reani-alei-protecao- dados-relacoes-trabalho Acesso em: 12 de março de 2021.

REIS, Beatriz de Felippe. O Direito Fundamental à Proteção de Dados Pessoais e Sensíveis do Trabalhador Frente às novas tecnologias da informação e comunicação. Universidade do extremo sul catarinense programa de pós-graduação em direito mestrado em direito Disponível em:

http://repositorio.unesc.net/bitstream/1/7469/1/Beatriz%20De%20Felippe%20Reis.pdf Acesso em: 12 de março de 2020.

REQUIÃO, Maurício. Covid-19 e proteção de dados pessoais: o antes, o agora e o depois. Disponível em https://www.conjur.com.br/2020-abr-05/direito-civil-atual-covid-19-protecao-dados-pessoais-antes-agora-depois Acesso em: 06 de março de 2021.

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679. Acesso em: 12 de março 2021.

SOUZA, Tercio Roberto Peixoto. A lei geral de proteção de dados pessoais (LGPD) no. 13.709/2019, a adequada custódia de dados pessoais na relação de emprego e o dever de indenizar do empregador. Disponível em: http://www.trabalhoemdebate.com.br/artigo/detalhe/por-tercio-souza-a-lei-geral-de-protecao-de-dados-pessoais-lgpd-lei-no-137092019-a-adequada-custodia-de-dados-pessoais-na-relacao-de-emprego-e-o-dever-de-indenizar-do-empregador. Acesso em: 12 de março 2021.

TEIXEIRA, Lucas. Teoricamente impossível: problemas com a anonimização de dados pessoais. Disponível em: https://antivigilancia.org/pt/2015/05/anonimizacao-dados-pessoais/ Acesso em: 12 de março de 2021.

PAMPLONA FILHO, Rodolfo; VASCONCELOS CONI JUNIOR, Vicente. A Lei Geral De Proteção De Dados Pessoais e Seus Impactos No Direito Do Trabalho. Disponível em: file:///C:/Users/aim/Downloads/6744-26372-1-PB.pdf Acesso em: 1º de abril de 2021.

DONEDA, Danilo Cesar Maganhoto. Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade. 2000. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/anexos/8196-8195-1-PB.htm. Acesso em: 31 de março de 2021.

SCHREIBER, Anderson. Proteção de dados pessoais no Brasil e na Europa. Jornal Carta Forense, 05 set. 2018. Disponível em: http://www.cartaforense.com.br/conteudo/colunas/protecao-de-dados-pessoais-no-brasil-e-na-europa/18269. Acesso em: 02 de abril de 2021.