DOI: 10.5433/2178-8189.2019v23n2p127

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E SEUS REFLEXOS NAS RELAÇÕES DE TRABALHO

GENERAL LAW ON DATA PROTECTION AND ITS REFLECTIONS ON WORK RELATIONS

Lara Castro Padilha Ramos*
Ana Virgínia Moreira Gomes**

Como citar: RAMOS, Lara Castro Padilha; GOMES, Ana Virgínia Moreira. Lei geral de dados pessoais e seus reflexos nas ralações de trabalho. **Scientia Iuris**, Londrina, v. 23, n. 2, p. 127-146, jul. 2019. DOI: 10.5433/2178-8189.2019v23n2p127. ISSN: 2178-8189

Resumo: A Lei n° 13.709, Lei Geral de Proteção de Dados Pessoais – LGPDP, promulgada em 14 de agosto de 2018 que entrará em vigor em 20 de fevereiro de 2020, regulamenta a proteção de dados pessoais, garante o exercício dos direitos da personalidade, e estabelece limites ao direito de acesso às informações de terceiros e à utilização de tais dados com intenções discriminatórias, ilícitas ou ilegais. O objetivo deste trabalho é analisar a nova lei, considerando se as suas diretrizes asseguram a efetiva proteção de dados pessoais nas relações de trabalho. A análise inicia-se com o exame do princípio constitucional da privacidade e sua evolução normativa, seguida dos fundamentos, princípios, objetivos e regras da LGPDP. A terceira seção analisa as repercussões jurídicas da nova norma para a proteção dos dados dos trabalhadores nas relações de trabalho. O método utilizado é descritivo-analítico e qualitativo, e a pesquisa realizada é bibliográfica, através de livros e artigos sobre o tema. O estudo sugere que a LGPDP trouxe uma gama de obrigações para as empresas, que terão de se adaptar e adotar medidas técnicas, administrativas e de segurança com vistas à proteção dos dados pessoais e sensíveis obtidos em decorrência das relações de trabalho.

Palavras-Chave: Princípio da privacidade. Proteção de dados. LGPDP. Direito do trabalho.

Abstract: Law No. 13,709, General Law for the Protection of Personal Data - LGPDP, promulgated on August 14, 2018 and will come into force on February 20, 2020, regulates the protection of personal data, guarantees the exercise of personality rights, and establishes limits to the right of access to the information of

*Mestrado e andamento em Direito pela Universidade de Fortaleza (UNIFOR)
Especialista em Direito em 2014 pelo Centro Universitário Christus NICHISTUS)
Graduada em Direito em 2005 pela Universidade de Fortaleza (UNIFOR)
E-mail: lara_castro_padilha@msn.com

**Doutora em Direito em 2000 pela Universidade de São Paulo (USP)
Mestrado em Faculty of Low em 2009 pela University of Toronto (UTORONTO)
Graduada em Direito em 1994 pela Universidade Federal do Paraná (UFC)
E-mail: avmgomes@gamail.com

third parties and the use of such data with discriminatory, illegal or illegal intentions. The purpose of this paper is to analyze the new law, considering whether its guidelines ensure the effective protection of personal data at work. The analysis starts with the exam of the constitutional privacy principle and its normative evolution, following by the study of the LGPDP principles, objectives and rules. The third section analyzes the legal repercussions of the new norm for the protection of workers' data at work. The method used is descriptive-analytical and qualitative, and the research is bibliographical, through books and articles on the subject. The study suggests that the LGPDP has brought a range of obligations for companies, which will have to adapt and adopt technical, administrative and security measures for the protection of personal and sensitive data obtained through the labor relation.

Keyword: Principle of privacy. Protection of data. General Law of Protection of Personal Data. Labor law.

INTRODUÇÃO

O atual cenário do desenvolvimento tecnológico facilitou o acesso às informações pessoais, inclusive a dados sensíveis, tanto pelo poder público quanto por entes privados, justificando a necessidade do desenvolvimento de novas formas de proteção da vida privada. No Brasil, essa necessidade veio a ser suprida pela promulgação da Lei Geral de Proteção de Dados Pessoais - LGPDP, Lei n° 13.709, em 14 de agosto de 2018. A lei entrará em vigor em 20 de fevereiro de 2020. Todavia, é importante que desde já a doutrina analise e reflita acerca de suas repercussões nos diferentes campos do direito. A Lei n° 13.709/2018, ao regulamentar a proteção de dados pessoais, garante o exercício dos direitos da personalidade, estabelecendo limites ao direito de acesso às informações de terceiros e à utilização de tais dados com intenções discriminatórias, ilícitas ou ilegais. O objetivo deste trabalho é analisar a nova lei, considerando se as suas diretrizes asseguram a efetiva proteção de dados pessoais nas relações de trabalho.

É neste sentido que se encontram os problemas a serem estudados. Esta pesquisa considera como se desenvolveu o instituto da proteção de dados e qual sua correlação com o princípio constitucional da privacidade, quais os fundamentos, objetivos, princípios e principais normas da LGPDP; como ocorreu o desenvolvimento da proteção de dados nas relações de trabalho; quais os limites ao tratamento de dados nas relações de trabalho e quais as repercussões da LGPDP nas relações de trabalho.

Para tanto, dividiu-se o presente trabalho em três capítulos. No primeiro capítulo analisou-se os conceitos de privacidade e proteção de dados e seu surgimento e evolução na Europa e no Brasil. No segundo capítulo, examinou-se qual a fundamentação, os objetivos e princípios que nortearam a LGPDP e suas principais normas. No terceiro capítulo, debruçou-se sobre o desenvolvimento da proteção de dados nas relações de trabalho, os limites impostos ao instituto e as possíveis repercussões nas relações de trabalho provenientes da entrada em vigor da Lei n° 13.709/2018.

Fez-se uso da pesquisa descritiva-analítica e qualitativa sobre: a) o princípio constitucional da privacidade e a proteção de dados, bem como seu desenvolvimento no continente europeu e no Brasil; b) a LGPDP, seus fundamentos, objetivos, princípios e principais dispositivos e c) as possíveis repercussões da legislação nas relações de trabalho. Por fim, utilizou-se a pesquisa bibliográfica, através de livros e artigos o tema e as perspectivas da aplicação da legislação nas relações de trabalho.

1 PROTEÇÃO DE DADOS E O PRINCÍPIO CONSTITUCIONAL DA PRIVACIDADE

O direito à privacidade passa a ser construído teoricamente a partir das mudanças ocorridas na sociedade com a ascensão da burguesia no século XVIII. Tendo em vista a modernização do espaço urbano, diversas atividades passaram a ser exercidas de forma particular pela população - fato que motivou o início das reflexões acerca da noção de privacidade.

O estudo do direito à privacidade tem como marco doutrinário inicial o artigo *the right to privacy* de Brandeis e Warren publicado na Harvard Law Review. A partir do relato da divulgação não autorizada na mídia de fatos acerca do casamento da filha de Warren, os autores tratam da privacidade não somente em relação à vida privada, mas como forma de proteção da personalidade e segurança de uma pessoa, que teria o direito de estar só (BRANDEIS; WARREN, 1980, p. 193).

A princípio, a privacidade tem como principal característica o individualismo exacerbado, condicionado ao isolamento social do indivíduo. A partir da segunda metade do século XIX, com o apogeu do liberalismo jurídico clássico, a privacidade apresenta seu caráter social ao colaborar com a criação de limites a serem obedecidos pela sociedade a fim de respeitar a vida privada de cada indivíduo, tornando-se pré-requisito de outras liberdades fundamentais (DONEDA, 2006, p. 16).

Marcel Leonardi (2012, p. 79) menciona que doutrina e jurisprudência já produziram diferentes conceitos sobre privacidade, os quais podem ser enquadrados em quatro categorias, resumidas a seguir: o direito de ser deixado só; o resguardo contra interferências alheias; o segredo ou sigilo e o controle sobre informações e dados pessoais. Entretanto, o autor conclui pela necessidade de haver um conceito plural de privacidade do modo mais amplo possível, ante sua caracterização como direito fundamental e direito da personalidade, podendo a proteção de dados ser considerada uma faceta do direito à privacidade sob a perspectiva de direito da personalidade humana.

Paralelo à consolidação do direito à privacidade como direito fundamental, ao longo do tempo do século passado e no início deste, as informações pessoais passaram a se tornar fonte de vantagens para quem as detém, sejam tais vantagens pessoais ou econômicas. O armazenamento e uso adequado dessas informações conferem maior poder de uns sobre os outros (COSTA; GOMES, 2017, p. 220).

Esse é o contexto da sociedade da informação, que, segundo Manuel Castells (1999, p. 21), é uma sociedade na qual a tecnologia é considerada indispensável em todos os ramos sociais, inclusive para o desenvolvimento da própria informação e construção do conhecimento pelos indivíduos, tendo como base ideal os valores de liberdade e comunicação. Forma-se uma nova estrutura social, de uma sociedade em rede. O crescimento do fluxo de informações aumentou o dinamismo da sociedade e, rapidamente, a captação de informações, dados pessoais, tornou-se estratégia interessante tanto para o Estado quanto para os entes privados com o objetivo de conhecer de forma aprofundada seus indivíduos e consumidores ou trabalhadores, respectivamente.

O interesse do Estado em adquirir informações está diretamente relacionado ao princípio da eficiência e do controle social, utilizando-se de pesquisas e censos para obtenção de maior conhecimento sobre a população e consequente aumento de seu poder de controle sobre os indivíduos. Já a importância da coleta de dados para os entes privados se evidencia a partir do desenvolvimento de tecnologias que diminuem o custo da coleta e tratamento de dados, transformando tais informações em utilidade para as empresas das mais diversas áreas de atuação, em especial às com fins comerciais e, na atualidade, com importante enfoque nas relações de

trabalho (DONEDA, 2006, p. 8).

Em âmbito internacional, a Declaração Universal dos Direitos do Homem de 1948 – DUDH em seu artigo 12[1] assegura o direito de todos terem sua vida privada resguardada sem interferências ou ataques de terceiros. O Pacto Internacional dos Direitos Civis e Políticos – PIDCP, ratificado pelo Brasil mediante Decreto 592 de 06 de julho de 1992, em seu artigo 17[2], garante o direito à privacidade. Em âmbito nacional, o direito à privacidade é espécie do gênero dos direitos da personalidade, regulados pelo Código Civil Brasileiro – CCB, precisamente em seu artigo 21[3] que trata da vida privada, e resguardados pela Constituição da República Federativa do Brasil de 1988 em seu artigo 5°, inciso X[4], que garante o direito à vida privada como direito fundamental.

O conceito de intimidade diz respeito às relações subjetivas e de trato íntimo da pessoa humana, suas relações familiares e de amizade. Já o conceito de vida privada abrange a intimidade, envolvendo todos os relacionamentos de uma pessoa, não só pessoais, mas também comerciais, trabalhistas, financeiras, dentre outras. Por privacidade entende-se o direito à manutenção de informações pessoais e da própria vida pessoal, definição das informações que podem ou não podem ser expostas. Pode ser também entendida como o controle de sua própria exposição e disponibilidade de informações acerca de si mesmo. A utilização do termo privacidade foi selecionada nesse artigo devido ao fato de ser gênero, abordando de forma ampla as espécies intimidade e vida privada (DONEDA, 2008, p.1).

A evolução do significado de privacidade na sociedade reflete no modo como o direito à privacidade deixa de se estruturar entre pessoa, informação e segredo para se estruturar entre pessoa, informação, circulação e controle. Com o advento do avanço tecnológico, o fluxo de informações e dados pessoais disponibilizados para terceiros é enorme e, a partir da perspectiva de proteção à vida privada e aos direitos de personalidade, o enfoque da privacidade como um direito egoísta e de individualismo exacerbado foi esfacelando-se (DONEDA, 2006, p. 14).

A utilização de dados pessoais coletados por instrumentos tecnológicos apresenta riscos aos seus proprietários, uma vez que possibilita a utilização indevida por parte de terceiros, pessoas físicas ou jurídicas. Por esse motivo, normas sobre a proteção de dados vêm sendo adotadas em países com vistas à proteção da pessoa humana e seu direito à privacidade; por exemplo, na Alemanha, Espanha, Portugal, dentre outros na Europa e nos Estados Unidos (DONEDA, 2006, p. 15).

Entende-se por proteção de dados ou autodeterminação informativa a autonomia de cada indivíduo para utilizar seus próprios dados como desejar, em conjunto com uma série de garantias estabelecidas para se evitar que esses dados sejam utilizados de forma discriminatória

1 Artigo 12 – "Ninguém será objeto de ingerências arbitrárias em sua vida privada, sua família, seu domicílio ou sua correspondência, nem de ataques a sua honra ou a sua reputação. Toda pessoa tem direito à proteção da lei contra tais ingerências ou ataques".

2 Artigo 17 – "Ninguém será objeto de ingerências arbitrárias ou ilegais em sua vida privada, sua família, seu domicílio ou sua correspondência, nem de ataques ilegais a sua honra e reputação. 2. Toda pessoa tem direito à proteção da lei contra essas ingerências ou esses ataques".

3 Artigo 21 – "A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma".

4 Artigo 5°, X – "São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito de indenização pelo dano material ou moral decorrente de sua violação".

de modo a causar danos de quaisquer espécies aos indivíduos ou à coletividade. A Convenção 108 do Conselho da Europa conceitua a proteção de dados como quaisquer informações relativas a um indivíduo que possa ser identificado. O direito à proteção de dados é expressão da liberdade e dignidade e relaciona-se com a proteção da própria personalidade. A proteção de dados se destina a regular a utilização da informação pessoal durante sua submissão em quaisquer redes, pois é necessário encontrar equilíbrio entre a preservação da privacidade e os instrumentos tecnológicos e sua ampliação a cada inovação.

No âmbito dessa proteção, certas categorias de dados especiais, como os de natureza médica e genética, não podem ser utilizados para fins negociais, pois o indivíduo não deve ser transformado em objeto sob vigilância constante (RODOTÁ, 2008, p. 19). São considerados dados sensíveis informações pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, bem como dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural, a fim de controlar e manipular seus cidadãos ou clientes e trabalhadores, respectivamente.

Com o objetivo de limitar o uso de dados pessoais por terceiros e garantir o controle e a proteção dos dados por parte de seu titular, princípios gerais basilares sobre proteção de dados foram estabelecidos. Dentre esses, listam-se os princípios da finalidade, da transparência ou publicidade, da adequação, do livre acesso, da necessidade e da qualidade de dados.

O princípio da finalidade determina que a coleta de dados ocorra somente quando seu uso e finalidade forem específicos, legítimos e explícitos. O princípio da transparência ou publicidade expõe a obrigatoriedade do fornecimento de informações claras e precisas aos titulares dos dados pessoais. Já o princípio da adequação dispõe sobre a imprescindibilidade de adequação e relevância no tratamento de dados de acordo com as expectativas do titular.

A garantia de consulta descomplicada e gratuita é premissa do princípio do livre acesso. O princípio da necessidade está diretamente relacionado à limitação do tratamento de dados ao mínimo necessário para a realização de suas finalidades. Por fim, a qualidade dos dados os mantém sempre atualizados e claros em consonância com o princípio da finalidade dos dados, facilitando sua detecção.

Alicerçado nos princípios basilares de proteção de dados, o tratamento autônomo da proteção de dados tem se desenvolvido doutrinaria e jurisprudencialmente por quatro décadas, iniciando-se na década de 60 (BRASIL, 2010, p. 40). Durante esse período diferentes gerações de normas foram adaptadas de um enfoque restrito para um mais geral com técnicas mais específicas aplicáveis às tecnologias adotadas para o tratamento de dados. As leis de proteção de dados foram desenvolvidas em decorrência da necessidade dos países em delinear qual o limite das informações pessoais que podem ser públicas e que devem permanecer privadas.

A Europa é considerada pioneira quando se trata da proteção de dados e sua regulamentação. A Alemanha foi o primeiro país europeu a formular uma lei sobre proteção de dados – a *Datenschutzgesetz,* Lei de Proteção de Dados -, em 1970, o que, posteriormente, impulsionou

a proteção do tema em âmbito nacional, intitulada de *Bundesdatenschutzgesetz*, Lei Federal de Proteção de Dados, no ano de 1979. Em 1983, o Tribunal Constitucional Alemão reconheceu o direito à autodeterminação informativa (FORTES, 2016, p. 154).

Após 23 anos da publicação da primeira legislação acerca da proteção de dados, em 1993, o continente europeu organiza-se em um bloco econômico, político e social denominado União Europeia – UE. A UE possui instrumentos legais para efetivar o cumprimento de suas decisões, diretivas e regulamentos por parte dos Estados-membros signatários. Nesse contexto, foi aprovada a Diretiva 95/46/CE sobre a proteção de dados, em 24 de outubro de 1995, com objetivo de se obter tratamento equivalente sobre a temática dentre os Estados-membros da UE.[5]

A Diretiva 95/46/CE trata sobre o conceito de dados pessoais, que alcançam não somente informações textuais, como também fotografias, imagens audiovisuais e registros de sons relacionados a certa pessoa. No conceito de proteção, inclui-se que essa seja feita também para pessoas póstumas. A diretiva estabelece princípios sobre a proteção de dados pessoais como lealdade, licitude e transparência, limitação à finalidade, adequação, exatidão, necessidade e duração da retenção de dados e segurança; disciplina sobre o consentimento e as hipóteses de vedação, como regra geral, ao tratamento de dados sensíveis, os que revelam origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, filiação sindical e dados relativos à saúde e vida sexual; discorre sobre os direitos do titular de dados e a proibição da transferência internacional de dados.

Em 2016, foi aprovado o Regulamento Geral sobre Proteção de Dados 679, que entrou em vigor no dia 25 de maio de 2018, reformulando a legislação de proteção de dados do continente europeu, de forma a revogar a Diretiva 95/46/CE.[6] A reforma foi proposta com base no caráter geral e vinculante que os regulamentos apresentam para todos os seus elementos, objetivos e meios, com o propósito de uniformizar os meios de aplicação das regras estabelecidas, além de ajustar a legislação às mudanças de conjuntura na sociedade ocasionadas pelo acesso à informação na atualidade.

A base do Regulamento 679 continua praticamente idêntica à base da diretiva 95/46/CE com manutenção de boa parte do texto da diretiva. O novo regulamento aplica-se ao tratamento de dados pessoais das pessoas físicas, independentemente da sua nacionalidade ou do seu local de residência, e por meios automatizados ou não automatizados de dados pessoais contidos ou destinados no contexto das atividades de um estabelecimento. A inovação ocorre em relação ao aumento da restrição de tratamento de dados, tornando-se mais recorrente a necessidade de consentimento e à restrição sobre o consentimento de menores de 16 anos de idade, que deverá ser feito pelos responsáveis do menor.

No Brasil, o texto constitucional prevê a hipótese de proteção da privacidade e dados

5 Os Estados-membros devem buscar alcançar o objetivo estabelecido na Diretiva, mas possuem discricionariedade para determinar quais meios serão utilizados na investida de seu cumprimento. Ressalta-se que a diretiva deve ser internalizada na legislação nacional dos países signatários dentro do prazo determinado em seu texto.

6 O Regulamento vincula tanto os objetivos estabelecidos quanto o meio que deve ser utilizados para alcançar sua finalidade.

pessoais em seu artigo 5°, inciso LXXII[7], através do habeas data, que é o remédio constitucional utilizado para assegurar ao impetrante conhecimento de quais dados pessoais encontram-se à disposição de órgãos públicos ou para a ratificação desses dados. Danilo Doneda (2006, p. 104) afirma, porém, que a ação constitucional não possui instrumentos suficientes para torná-la eficaz de modo a garantir a proteção de dados pessoais.

A Lei de Acesso à Informação, Lei n° 12. 527/2011 é a primeira legislação acerca do tratamento de dados e da internet e regulamentou o inciso XXXIII do artigo 5°[8] da Constituição, assegurando o direito fundamental de acesso às informações produzidas e armazenadas por órgãos públicos de todas as esferas.

Foram introduzidas, por meio da Lei de Acesso à Informação, garantias de direito à informação sobre dados institucionais dos órgãos e entidades do Poder Executivo Federal; dados gerais para o acompanhamento de programas e ações de órgãos e entidades; inspeções, auditorias, prestações e tomadas de contas realizadas pelos controles interno e externo; registros de quaisquer repasses ou transferências de recursos financeiros; registros das despesas; procedimentos licitatórios; formas de solicitação de informações[9].

Destaca-se a regra geral de obrigatoriedade de consentimento para acesso ou divulgação de dados com exceção de casos como: cumprimento de ordem judicial, direitos humanos, e pesquisas científicas que sejam de cunho relevante à sociedade com interesse público ou geral, casos nos quais o interesse público deve sobrepor-se ao interesse privado. Para complementar a Lei de Acesso à Informação, em 2012, foi promulgada a Lei n° 12.373 que versa sobre crimes cibernéticos, destacando-se o crime de invasão de dispositivo informático, tipificado no artigo 154-A do Código Penal, que reforça a preocupação do legislador com a proteção de dados pessoais.

Em 2014, após debates entre o governo e sociedade sobre a necessidade de regulação mais específica e atualizada sobre a matéria, a Lei n° 12.965, denominada de Marco Civil da Internet, foi promulgada, estabelecendo princípios, garantias, direitos e deveres para o uso da internet no país. Segundo Vinícius Borges Fortes (2016, p. 120), o marco civil representa o maior avanço normativo brasileiro relacionado ao uso da internet, reconhecendo direitos aos cidadãos dentro do contexto da internet.

Os pilares do Marco Civil da Internet são a neutralidade da rede, a privacidade e a liberdade de expressão. A Lei n° 12.965/2014 versa sobre os direitos dos usuários da internet com ênfase na proteção da privacidade e vida privada, conforme artigo o 7°, inciso I[10], e na proteção de dados pessoais, em seu artigo 3°, inciso III[11]. Por não ser uma legislação específica sobre proteção

7 Artigo 5°, LXXII - "Conceder-se-á habeas data: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo.

8 Artigo 5°, XXXIII – "Todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado".

9 Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.

10 Artigo 7° - "O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação".

11 Artigo 3° - "A disciplina do uso da internet no Brasil tem os seguintes princípios: III - proteção dos dados pessoais, na forma da lei".

de dados, muitos conceitos não foram demarcados. Dessa forma, o Decreto 8.771/2015 surgiu para regulamentar o Marco Civil da Internet e tutelar sobre a proteção e tratamento de dados, mas apresentou-se silente em relação ao conceito de dados pessoais.

Dada a insuficiência do sistema normativo, em 2018, a partir das diretrizes europeias sobre regulamentação de proteção de dados, o Brasil publicou a LGPDP, Lei n° 13.709, que altera o Marco Civil da Internet e trata sobre a proteção de dados de forma específica.

2 A Lei Geral de Proteção de Dados Pessoais

A LGPDP, Lei n° 13.709 de 14 de agosto de 2018, é a legislação brasileira que determina como os dados pessoais dos cidadãos podem ser coletados e tratados e quais punições, decorrentes de eventuais transgressões, devem ser aplicadas. A lei de proteção de dados cria um vínculo jurídico entre o indivíduo e seus dados, justificado pela identidade da informação, isto é, dos dados com a pessoa.

A partir da vulnerabilidade de dados pessoais disponibilizados, mormente os expostos na internet, o governo brasileiro optou por criar legislação específica sobre a proteção de dados pessoais. A LGPDP adveio do Projeto de Lei 53/2018, que se baseou nas diretrizes do Regulamento Geral sobre a Proteção de Dados da União Europeia, e, após aprovação nas duas casas legislativas, foi sancionado pelo Presidente da República em exercício, Michel Temer. A lei passará a ter eficácia em 15 de fevereiro de 2020 em todo território nacional, ou seja, determinou-se período de 18 meses para adaptação do governo, empresas e sociedade.

A LGPDP 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. Baseia-se na livre iniciativa, no desenvolvimento econômico e tecnológico do país, em consonância com a dignidade e o exercício da cidadania.

Dentre os princípios da LGPDP, destacam-se o da finalidade, adequação, necessidade, livre acesso, qualidade de dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas. Segundo o princípio da finalidade, os dados somente devem ser utilizados para as finalidades específicas para as quais foram coletados e informados aos seus titulares. O princípio da adequação trata da compatibilização do uso dos dados com a finalidade informada. A limitação do uso do dado ao mínimo necessário para se atingir a finalidade desejada reflete o princípio da necessidade.

O livre acesso relaciona-se com as garantias, aos titulares dos dados, de informações facilitadas, que devem ser disponibilizadas de forma gratuita, caso haja requerimento por parte do titular. A qualidade de dados garante exatidão, clareza, relevância e atualização dos dados. Já o princípio da transparência deve ser aplicado no intuito de oferecer dados claros e precisos sobre a realização do tratamento e agentes de tratamento. O princípio da segurança visa à proteção dos dados de acesso pessoais não autorizados e de situações acidentais ou ilícitas de destruição, perda,

alteração, comunicação ou difusão de dados.

O princípio da prevenção decorre da adoção de medidas com o objetivo de precaver a ocorrência de danos em virtude do tratamento de dados pessoais. O princípio da não discriminação impossibilita que os dados sejam usados para fins discriminatórios, ilícitos ou abusivos. Por fim, a responsabilização e prestação de contas devem ocorrer fundamentadas na demonstração da adoção de medidas eficazes e capazes de comprovar o cumprimento das normas de proteção de dados por parte do agente.

De acordo com o artigo 17, a lei cita como seu destinatário "Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade". Dentre os direitos que o titular dos dados pessoais possui, destaca-se o direito de acesso, que garante a obtenção de todos os dados pessoais que estão sendo tratados, mediante requisição aos controladores e, em consequência, os direitos de retificação e atualização, haja vista a obrigação dos agentes de os manter sempre corretos e atualizados.

Ademais, citam-se, ainda, como direitos do titular de dados o direito de confirmação da existência de tratamento; de anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na lei; de portabilidade dos dados a outro fornecedor de serviço ou produto; de eliminação dos dados pessoais tratados com o consentimento do titular; de informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; de informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa e de revogação do consentimento, a ser realizada de forma gratuita[12].

O artigo 5° da legislação define dado pessoal como qualquer informação que identifique precisamente ou torne identificável uma pessoa natural, assim como nomes, domicílio, números de telefone, infrações administrativas e penais, dentre outras. A determinação da característica da pessoalidade de um dado advém da possibilidade de se identificar uma pessoa concretamente, diferenciando-o do restante da coletividade. Por sua vez, como já ressaltado, dado pessoal sensível é aquele que versa sobra a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, estado de saúde ou vida sexual de uma pessoa natural.

Por tratamento entende-se toda operação, automatizada ou não, realizada com dados pessoais, tais como a coleta, utilização, acesso, transmissão, processamento, arquivamento, armazenamento ou transferência. Qualquer operação de tratamento de dados pessoais realizada no território nacional, por pessoa natural ou pessoa jurídica de direito público ou privado, cujos titulares estejam localizados no Brasil, ou que tenha por finalidade a oferta de produtos ou serviços no Brasil, estão sujeitos à LGPDP, que passa a exigir o consentimento expresso do usuário para esta operação[13] (BRASIL, 2018).

O artigo 4° da lei lista exceções à aplicação ao tratamento de dados pessoais, quais sejam

12 Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm.
13 Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm.

as hipóteses de tratamento de dados pessoais realizado por pessoa natural para fins exclusivamente particulares e não econômicos e os realizados exclusivamente para fins jornalístico, artístico ou acadêmico; de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais e de dados em trânsito, ou seja, aqueles que não tem como destino agentes de tratamento no Brasil[14] .

O consentimento deve ocorrer por manifestação livre e inequívoca do titular, por escrito, expressando sua concordância com o tratamento de seus dados pessoais para uma finalidade determinada, não sendo admitidas autorizações genéricas, sendo vedado o tratamento, caso a autorização tenha sido obtida mediante vício de consentimento.

Denota-se a criação de agentes de tratamento de dados pessoais, denominados controlador e operador, que podem ser uma pessoa natural ou jurídica, de direito público ou privado. Exercem a função de manter o registro das operações de tratamento de dados que realizarem, sendo função do controlador, especificamente, decidir sobre o tratamento de dados pessoais, enquanto a função exercida pelo operador é a realização do tratamento por ordem do controlador.

Conforme o artigo 46, os agentes de tratamento devem adotar medidas de segurança, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Qualquer incidente deve ser comunicado à autoridade nacional, órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento da lei, e à vítima, titular dos dados, em prazo razoável e com descrição minuciosa dos dados afetados e indicação das medidas técnicas e de segurança utilizadas, bem como as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

A criação da autoridade nacional foi vetada pelo Poder Executivo, pois implicaria em inconstitucionalidade do processo legislativo por trazer vício de iniciativa, uma vez que a iniciativa pertence ao Presidente da República, que já sinalizou concordância com a criação do órgão, e que enviará um projeto de lei para essa finalidade.

Outro aspecto relevante é o fluxo de dados para outros países, a chamada transferência internacional de dados, que somente será permitida para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais compatível com a lei brasileira ou mediante oferecimento de garantias do regime de proteção de dados local.

As empresas ficam responsáveis por, através de seus agentes de tratamento, elaborar relatório de impacto à proteção de dados pessoais, com descrição dos tipos de dados coletados, o fundamento da coleta e a metodologia utilizada para a coleta e garantia da segurança das informações, no que resulta na importância da contratação e consultoria de empresas especializadas em segurança da informação confiáveis.

Isto posto, percebe-se importante papel a ser exercido pelas empresas em relação à proteção de dados pessoais. A seguir, serão apontadas possíveis repercussões normativas provenientes da LGPDP nas relações de trabalho.

14 Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm.

3 REPERCUSSÕES NORMATIVAS DA LEI GERAL DE PROTEÇÃO DE DADOS NAS RELAÇÕES DE TRABALHO

A relação entre trabalho e tecnologia tem início com a evolução de ferramentas utilizadas para o mercado agrícola e a transferência da força humana para as máquinas com o advento da Revolução Industrial. O objetivo da inserção da tecnologia no mercado de trabalho foi o de aumentar a produtividade, facilitar e melhorar as condições de trabalho humano, bem como promover, em teoria, maior disponibilidade de tempo livre para os trabalhadores (GOOS, 2018, p. 2). Na atualidade, vivencia-se a revolução informacional, modelo de desenvolvimento que privilegia o uso da tecnologia (CASTELL, 1999, p. 21).

As relações de trabalho e as formas de trabalho vêm se adaptaram às mudanças tecnológicas e sua constante evolução no mercado. O progresso tecnológico e o acesso mais rápido a informações tiveram papel relevante e benéfico, pois possibilitaram o uso de instrumentos tecnológicos pelo trabalhador, facilitadores da execução das atividades laborais, tornando o trabalho mais ágil e menos dispendioso em relação ao tempo, gerando maior produtividade e lucratividade para as empresas. Em contrapartida, essas ferramentas tecnológicas permitiram ao empregador um maior controle e vigilância sobre os empregados, afetando o modo como o poder diretivo pode ser exercido (COSTA; GOMES, 2017, p. 223).

Segundo Maurício Godinho Delgado (2002, p. 608), o poder empregatício é o poder exercido pelo empregador sobre seus empregados e divide-se em poder diretivo, regulamentar, disciplinar e fiscalizatório. O poder diretivo é o poder exercido pelo empregador a fim de organizar sua empresa em relação às atividades, funções e cargos a serem desenvolvidos. O regulamentar caracteriza-se pelos meios formais e informais utilizados para concretizar o poder diretivo. Já o poder disciplinar permite punição aos trabalhadores que violem normas de contrato de trabalho e, por último, o poder fiscalizatório é aquele que permite ao empregador verificar e acompanhar as atividades de seus empregados.

O poder fiscalizatório do empregador, em razão do progresso da informática, passou a contar com novos instrumentos para o seu exercício, que o tornam mais constante e evidente. Incluem-se no monitoramento eletrônico, por exemplo, o monitoramento de e-mails e vídeos, o rastreamento de computadores e localização dos trabalhadores, uso do telefone, os sítios navegados pelos empregados. A partir de uma base de dados conhecida como "big data", é desenvolvido um sistema que analisa grande quantidade de dados para revelar padrões ocultos que podem auxiliar na tomada de decisões empresariais futuras e imediatas (STEFANO, 2018, p. 15). A partir do uso da "big data", iniciou-se a utilização de processo ou método de gestão de recursos humanos para capturar estimativas de desempenho no trabalho denominada "people analytics".[15]

Segundo Jorge Luiz Souto Maior (2006, p. 92), apesar de, sob a ótica da filosofia moderna, o trabalho dignificar o homem; contraditoriamente, a utilização da tecnologia no ambiente de trabalho pode retirar a dignidade humana, impondo restrições aos direitos de personalidade do

15 Para um levantamento da literatura sobre o tema, ver Giacumo; Breman (2016).

empregado na medida em que a tal tipo de fiscalização no trabalho pode interferir e desrespeitar sua intimidade e privacidade. A obtenção de informações importantes acerca da vida dos indivíduos passou a ser facilmente adquirida. O controle de e-mails, informações disponibilizadas em redes sociais e a utilização de aplicativos de conversas *online*, que facilitam a comunicação constante entre as pessoas, são benéficos em termos gerais, mas maléficos para as relações de trabalho caso utilizados sem ponderação por parte dos empregadores, circunstância que pode acentuar o desequilíbrio entre as partes nas relações de trabalho.

Empregadores, movidos pela revalorização do caráter pessoal nas relações de trabalho, valem-se de tratamento de dados pessoais de candidatos a postos de trabalho e de trabalhadores que servem de critérios para decisões sobre contratação, manutenção da relação laboral, promoções ou desligamento da empresa. Em certas situações, o trabalhador ou candidato é invadido em sua privacidade, sendo avaliado por características pessoais que não se referem à qualificação necessária para a função a ser exercida. Até mesmo sem o conhecimento do trabalhador, o levantamento dos dados pessoais pode levar à violação de direitos fundamentais do trabalhador. Citam-se como exemplos de excessivos levantamentos de dados pessoais a aplicação de testes genéticos, exames toxicológicos, questionamentos sobre orientação sexual e opinião política em casos de seleção de empregados. Além do levantamento para uso da própria empresa, os dados do empregado podem ser vendidos pela empresa, o que constitui outro exemplo de invasão de privacidade.

Valerio de Stefano (2018) cita que regras e negociações coletivas acerca do tema são essenciais para estancar casos abusivos, tais quais, recrutamentos a partir da utilização de dados pessoais, aplicados, mormente, nas contratações nas quais o trabalho requer relação de confiança mais intensa entre empregador e empregado. A contratação de trabalhadores domésticos na função de cuidar de crianças, por exemplo, que envolva a captação de dados pessoais e análise de personalidade por programas que conseguem determinar, a partir das informações coletadas, os riscos (probabilidade de envolvimento com drogas, linguagem e utilização de mídias inapropriadas, dentre outras) que o trabalhador pode oferecer à criança.

A aplicação da LGPDP é essencial para resgatar o equilíbrio na relação de trabalho entre empregador e empregado a partir da necessidade de autorização para coleta de dados por parte do trabalhador e da imposição de limites ao tratamento de dados no âmbito das relações laborais que garantam o respeito aos direitos fundamentais à privacidade, proteção de dados, liberdade e dignidade humana dos trabalhadores. Outrossim, devem ser aplicados os princípios do Direito do Trabalho e considerado o Repertório de Recomendações Práticas da Organização Internacional do Trabalho[16] (OIT, 2019) , que trata sobre a proteção de dados dos trabalhadores.

O Repertório de Recomendações e Práticas de Proteção de Dados dos Trabalhadores fora implementado em 1997 pela Organização Internacional do Trabalho com o propósito de fornecer orientação sobre a proteção de dados pessoais do trabalhador, estabelecendo preceitos

16 Disponível em: https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf

como o processamento de dados de forma legal e justa e somente quando relevante para o emprego do trabalhador; utilizado apenas para o propósito inicialmente determinado e, em caso de processamento para fins diversos do incialmente estabelecido, garantir sua compatibilidade com a finalidade original, bem como evitar interpretações errôneas; a não utilização de dados coletados para controlar o comportamento dos trabalhadores; não vinculação dos dados coletados com o desempenho do trabalhador; informação aos trabalhadores sobre quaisquer processos de coleta de dados a seu respeito; a não utilização de dados como justificativa para quaisquer tipos de preconceito e discriminação; a não renúncia dos trabalhadores aos seus direitos e a necessidade de uma clausula de confidencialidade por parte de quem manipula e coleta tais dados (OIT, 2019).

A Lei Geral de Proteção de Dados, publicada em 14 de agosto de 2018, entrará em vigor em 15 de fevereiro de 2020, fazendo-se necessária a análise dos possíveis impactos que causará nas relações de trabalho como em processos seletivos, prática de armazenamento de currículos, repasse de dados a terceiros, sindicatos e ao poder público, bem como o tratamento de dados a ser realizado por ele. Do sistema da LGPDP, deduz-se inicialmente duas regras gerais a serem aplicadas nas relações de trabalho: primeiro, a regra de proteção aos dados sensíveis do trabalhador; segundo, a regra do consentimento, conforme a qual o empregador deve informar ao trabalhador a realização de levantamento de dados, assim como as consequências do consentimento e fornecimento de tais informações.

No que concerne à proteção aos dados sensíveis, a regra geral é a de que o trabalhador de não terá realizado o tratamento de seus dados especialmente protegidos, isto é, os dados sensíveis. Somente em casos nos quais há o conhecimento de tais dados constitui informação essencial para a realização da atividade. Por exemplo, casos de trabalhos nos quais se enquadrem em atividade de risco, sendo necessário o conhecimento do quadro clínico de saúde do trabalhador, como cumprimento de norma de segurança laboral, para verificar se esse apresenta condições de exercer o a atividade mediante condições adversas. Deve-se demonstrar, portanto, interesse legítimo para acesso aos dados sensíveis, justificando a renúncia pontual do empregado em relação à proteção de seus dados.

A segunda regra trata da necessidade de o empregador informar ao trabalhador ou candidato ao emprego se coletas de dados serão feitas, bem como informar as consequências do consentimento e fornecimento de tais informações. Tendo em vista a extrema importância do direito ao consentimento, limites a esse também são aplicáveis. Devido à hipossuficiência do trabalhador ou mesmo candidato nas relações de trabalho, nem sempre seu consentimento será espontâneo. Neste sentido, existem limites gerais às regras de consentimento que partem da consideração realista da situação ao observar-se os desníveis existes entre empregado ou candidato e empregador, que podem, porventura, inibir sua liberdade de escolha (FONS, 2005, p. 39). As hipóteses de dispensa de consentimento devem ser previamente estabelecidas entre empregador e empregado, uma vez que algumas situações dispensam a exigibilidade de consentimento do empregado como, por exemplo, a coleta de dados essenciais à continuidade da relação de trabalho ou para o cumprimento do contrato (FONS, 2005, p. 40).

A seguir serão examinadas hipóteses especificas de utilização de dados dos trabalhadores pela empresa que potencialmente incompatíveis com o sistema estabelecido pela LGPDP.

A responsabilidade das empresas, no Direito do Trabalho, existe antes mesmo de consolidação de vínculo empregatício, ou seja, já na fase pré-contratual, durante o processo seletivo. Um dos princípios basilares da LGPDP é o da não discriminação, não podendo uma pessoa ser prejudicada a partir de informações constadas em seus dados pessoais. Portanto, em processos seletivos, devem ser evitados anúncios que exijam requisitos conceituados pela legislação, especialmente, como dados sensíveis, por exemplo, estipular qual o gênero da pessoa, estado civil, religião, opção sexual, de forma injustificada. No mesmo sentido, já dispunha a Lei n° 9.029 de 13 de abril de 1995, que proíbe a exigência de atestados de gravidez e esterilização, e outras práticas discriminatórias, para efeitos admissionais ou de permanência da relação jurídica de trabalho.

A discriminação em processo seletivo com base em dados pessoais ofende os direitos humanos do candidato, bem como o princípio constitucional da dignidade da pessoa humana, contido no artigo 1°, inciso III da Constituição; direitos constitucionais como inviolabilidade à vida, à liberdade e à igualdade, bem como à intimidade e à vida privada, respectivamente no artigo 5°, caput e inciso X da Constituição ; o objetivo fundamental da República Federativa do Brasil, expresso em seu artigo 3°, inciso IV, de promover o bem de todos, sem preconceitos de raça, sexo, cor, idade e quaisquer outras formas de discriminação.

Também ofende o direito social ao trabalho, artigo 6° da Constituição; além de direitos trabalhistas que vedem a discriminação como a proibição de critérios de admissão por motivo de sexo, cor, idade ou estado civil e discriminação de salários, contidos no artigo 7° da Constituição. A escolha de critérios para seleção de candidatos a um posto de trabalho, especialmente em relação aos dados pessoais solicitados aos candidatos, deve se pautar por essas normas. O setor de recursos humanos das empresas deve ter treinamento adequado para desenvolver critérios e práticas não discriminatórias.

Outra repercussão que pode vir à tona a partir da vigência da LGPDP é a prática de armazenamento de currículos em banco de dados, pelas empresas, a serem utilizados em seleções posteriores. As empresas terão de solicitar o consentimento dos candidatos para que possam mantê-los e utilizar-se dessa prática tão comum com vistas à segurança das informações pessoais contidas nos bancos de dados. Outrossim, dados relativos a qualificações profissionais podem ser utilizados com o escopo de beneficiar, proporcionar vantagens ao trabalhador, devendo ser pautados no princípio da finalidade, ou seja, a finalidade do tratamento de dados deve ser legítima e restrita ao assunto laboral determinado no caso concreto.

No caso de empresas que oferecem serviços de plano de saúde, seguro de vida, dentre outros aos seus empregados, os contratos de trabalho deverão conter cláusulas específicas sobre a proteção de dados pessoais, pois as empresas não poderão repassar dados de seus empregados a terceiros sem autorização, tornando-se necessária, inclusive, revisão dos contratos entre as empresas e essas prestadoras de serviço a fim de atualizarem os contratos em consonância com a

LGPDP.

O envio de informações sobre empregados para sindicatos também irá requerer cautela, devendo-se verificar se há previsão em lei ou norma coletiva ou consentimento do empregado desde que seja demonstrada finalidade, necessidade e adequação específicas para que a transmissão de dados ocorra.

Em relação ao tratamento de dados pelo poder público, a LGPDP o permite desde que atendida a finalidade pública na persecução do interesse público. Tânia Gonçalves e Marcello Varella (2018, p. 519) ressaltam a antinomia existente, nos casos que envolvam o tratamento de dados pelo poder público, do princípio constitucional da publicidade, pautado pelo acesso à informação, e do princípio constitucional da privacidade, que abrange a intimidade, a vida privada, a honra e a imagem. Como ambos são princípios constitucionais não há hierarquia entre os mesmos, e, ainda que a regra geral seja a prevalência do interesse público sobre o privado, deve-se haver solução sobre qual princípio deve prevalecer tão somente a partir da análise do caso concreto. Vieira (2002, p. 28) cita que só será justificável o interesse particular se sobrepujar sobre o público se não houver outra forma na qual o interesse em questão possa ser realizado.

Por fim, quanto à transmissão de dados de empresas para órgãos públicos, necessários para a execução de políticas públicas, como, por exemplo, envio de dados para declaração de Imposto de Renda – IR, recolhimento de valores referentes ao Fundo de Garantia por Tempo de Serviço – FGTS, para o Cadastro Geral de Empregados e Desempregados – CAGED ou Relação Anual de Informações Sociais – RAIS, não há necessidade de consentimento do empregado, pois são hipóteses previstas em lei.

CONCLUSÃO

A proteção de dados constitui uma forma de regular a utilização da informação pessoal durante seu tratamento, após o colhimento de tais dados, por meios eletrônicos ou não, para o poder público ou para esferas privadas, independentemente da utilização à qual sejam destinadas tais informações. A proteção de dados, além de fornecer proteção aos direitos constitucionais da liberdade, igualdade e vida privada, é uma forma indireta de proteção da pessoa e de sua dignidade.

A partir da percepção da necessidade de proteção das informações, normas foram elaboradas na tentativa de controlar tamanha difusão de dados, com potenciais efeitos negativos e discriminatórios. O continente europeu foi o pioneiro sobre a temática e regulamentação da matéria, destacando-se a Diretiva Europeia 95/46/CE que dispôs sobre os princípios para proteção de dados, quais sejam o princípio da finalidade, da transparência ou publicidade, da adequação, do livre acesso, da necessidade e da qualidade de dados.

No Brasil, a proteção de dados somente foi regulada em 2011 a partir da Lei de Acesso à Informação, Lei n° 12.527/2011, que regulamentou o inciso XXXIII do artigo 5° da Constituição da República Federativa do Brasil, assegurando o direito fundamental de acesso às informações

produzidas e armazenadas por órgãos públicos de todas as esferas. Para complementar a Lei de Acesso à Informação, em 2012, foi promulgada a Lei n° 12.373, que versa sobre crimes cibernéticos, destacando-se o crime de invasão de dispositivo informático, tipificado no artigo 154-A do Código Penal, que reforça a preocupação do legislador com a proteção de dados pessoais.

Em 2014, após debates entre o governo e sociedade sobre a necessidade de regulação mais específica e atualizada sobre a matéria, a Lei n° 12.965, denominada de Marco Civil da Internet, é promulgada, estabelecendo princípios, garantias, direitos e deveres para o uso da internet no país. Por não ser uma legislação específica sobre proteção de dados, importantes conceitos não foram demarcados. Dessa forma, o Decreto 8.771/2015 veio para regulamentar o Marco Civil da Internet e tutelar sobre a proteção e tratamento de dados, mas apresentou-se silente em relação ao conceito de dados pessoais.

A necessidade de legislação específica sobre o tema tornou-se imperativa e, em 2018, a partir das diretrizes europeias sobre regulamentação de proteção de dados, o Brasil publicou a LGPDP, Lei n° 13.709, que altera o Marco Civil da Internet e trata sobre a proteção de dados de forma específica.

O progresso tecnológico e o acesso mais rápido a informações tiveram papel relevante no desenvolvimento das atividades laborais, pois possibilitaram o uso de instrumentos tecnológicos pelo trabalhador, facilitadores da execução das atividades laborais, tornando o trabalho mais ágil por meio de tarefas que antes só podiam ser realizadas manualmente e com grande dispêndio de tempo, gerando maior produtividade e lucratividade para as empresas.

Em contrapartida, as relações de trabalho tornaram-se mais frágil do ponto de vista da exposição dos empregados a partir da captação de informações pelos empregadores, por meios eletrônicos, principalmente, uma vez que tais dados podem ser utilizados de forma estratégica para fins mercantis desde o conhecimento de características pessoais de empregados e candidatos a contratação, até suas atividades cotidianas, crenças religiosas e orientação sexual. Todos os dados podem ser operados para estimular contratação, manutenção da relação laboral ou desligamento de empresas.

A LGPDP trouxe uma gama de obrigações para as empresas, que terão de se adaptar e adotar medidas técnicas, administrativas e de segurança com vistas à proteção dos dados pessoais e sensíveis obtidos em decorrência das relações de trabalho. Dessa forma, é necessário planejamento para verificar se os contratos realizados entre empregadores, empresas e empregados, bem como entre empresas e prestadores de serviços, como empresas de planos de saúde, seguro de vida, dentre outros, estão em consonância com as exigências estabelecidas pela LGPDP; avaliar se os colaboradores também possuem noção de responsabilidade sobre as informações para evitar vazamentos de dados; buscar consultoria especializada em segurança da informação a fim de evitar penalidades administrativas ou ações de responsabilização civil por eventuais danos causados.

REFERÊNCIAS

BARROS, Juliana Augusta Medeiros de. **A utilização de Meios Eletrônicos no Ambiente**

de Trabalho: a colisão entre os direitos à intimidade e à privacidade do empregado e o poder diretivo do empregador. São Paulo: LTr, 2002.

BRASIL. Código Penal Brasileiro. **Decreto-Lei n° 2.848, de 7 de dezembro de 1940**. Código Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm . Acesso em: 06 novembro 2018.

_____. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 06 novembro 2018.

_____. **Decreto n° 8.771, de 11 de maio de 2016**. Regulamenta a Lei n° 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm>. Acesso em: 16 novembro 2018.

_____. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo: para além da informação creditícia / Escola Nacional de Defesa do Consumidor**; elaboração Danilo Doneda. – Brasília: SDE/DPDC, 2010.

_____. **Lei** n° 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5°, no inciso II do § 3° do art. 37 e no § 2° do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm >. Acesso em: 06 novembro 2018.

_____. **Lei n° 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 16 de novembro de 2018.

_____. **Lei n° 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 16 novembro 2018.

CASTELLS, Manuel**. A sociedade da informação: economia, sociedade e cultura - v. 1.** Lisboa: Fundação Calouste Gulbenkian, 1999.

COSTA, Andréa Dourado; GOMES, Ana Virginia Moreira. Discriminação nas relações de trabalho em virtude da coleta de dados sensíveis. **Scientia Iuris**, Londrina, v. 21, n. 2, p. 214-236, jul. 2017.

DACHERI, Emanueli; GOLDSCHMICDT, Rodrigo. O impacto da tecnologia nas relações de trabalho: uma análise à luz da teoria da eficácia horizontal dos direitos fundamentais inespecíficos dos trabalhadores. **Revista de direitos fundamentais nas relações do trabalho, sociais e empresariais**. São Paulo. v. 3, n. 2, p. 66-87, jul/dez. 2017.

DELGADO, Mauricio Godinho. **Curso de direito do trabalho**. São Paulo: Ltr, 2002.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**. Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011

_____. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

_____. Privacidade, vida privada e intimidade no ordenamento jurídico brasileiro. Da emergência de uma revisão conceitual e da tutela de dados pessoais. In: Âmbito Jurídico, Rio Grande, XI, n. 51, mar 2008. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=2460>. Acesso em 18 dezembro 2018.

FONS, Daniel Martínez. Tratamiento y protección de datos de los trabajadores en la relación de trabajo. In: **Derecho social y nuevas tecnologías**. Madrid: Consejo General del Poder Judicial, 2005.

FORTES, Vinícius Borges. **Os direitos de privacidade e a proteção de dados pessoais na internet**. Rio de Janeiro: Lumen Juris, 2016.

GIACUMO, Lisa A.; BREMAN, Jeroen. "Emerging evidence on the use of big data and analytics in workplace learning: a systematic literature review**." Quarterly Review of Distance Education**, vol. 17, no. 4, 2016, p. 21+. Academic OneFile, http://link.galegroup.com/apps/doc/A493448340/AONE?u=utoronto_main&sid=AONE&xid=19cffbd8. Accessed 13 Dec. 2018.

GONÇALVES, Tânia Carolina Nunes Machado; VARELLA, Marcello D. Os desafios da Administração Pública na disponibilização de dados sensíveis. **Revista Direito GV**. São Paulo. v. 14, n. 2, p. 513-536, maio/ago. 2018.

GOOS, Maarten. 2018. "The Impact of Technological Progress on Labour Markets: Policy Challenges." **Oxford Review of Economic Policy** 34 (3): 362-375.doi:10.1093/oxrep/gry002. http://resolver.scholarsportal.info/resolve/0266903x/v34i0003/362_tiotpolmpc.

LEONARDI, Marcel. **Tutela e privacidade na Internet**. São Paulo: Saraiva, 2012.
MANTOVANI JUNIOR, Laert. **O Direito Constitucional à Intimidade e à Vida Privada do Empregado e o Poder Diretivo do Empregador**. São Paulo: Ltr, 2010.

RODOTÁ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

SANDEN, Ana Francisca Moreira de Souza. **A proteção de dados pessoais do empregado no direito brasileiro.** São Paulo: Ltr, 2014.
SOUTO MAIOR, Jorge Luiz. Do Direito à desconexão do trabalho. **Revista do Departamento de Direito do Trabalho e da Seguridade Social**, São Paulo, v, 1, n. 1, p. 92, jan./jun. 2006.
STEFANO, Valerio de. Collective bargaining of platform workers: domestic work leads the way. **Regulating for globalization**. 10 dezembro 2018. Disponível em: <http://regulatingforglobalization.com/2018/12/10/collective-bargaining-of-platform-workers-domestic-work-leads-the-way/>. Acesso em: 19 dezembro 2018.

_____. Valerio de. "**Negotiating the algorithm**": Automation, artificial intelligence and labour

protection. Geneva: International Labour Organization, 2018.
Oficina Internacional del Trabajo. **Repertorio de recomendaciones prácticas sobre la protección de los datos personales de los trabajadores**. Disponível em: <http://www.ilo.org/public/libdoc/ilo/1997/97B09_118_span.pdf>. Acesso em: 29 nov. 2018.

PORTUGAL, Comissão Nacional de Proteção de Dados. **Convenção 108**. Disponível em: < https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm >. Acesso em: 06 novembro 2018.

VIEIRA, Sônia Aguiar do Amaral. **Inviolabilidade da vida privada e da intimidade pelos meios eletrônicos**. São Paulo: Juarez de Oliveira, 2002.

Como citar: RAMOS, Lara Castro Padilha; GOMES, Ana Virgínia Moreira. Lei geral de dados pessoais e seus reflexos nas ralações de trabalho. **Scientia Iuris**, Londrina, v. 23, n. 2, p. 127-146, jul. 2019. DOI: 10.5433/2178-8189.2019v23n2p127. ISSN: 2178-8189

Recebido em: 29/01/2019.

Aprovado em: 04/07/2019.