UNIVERSIDADE DO EXTREMO SUL CATARINENSE – UNESC
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
MESTRADO EM DIREITO

BEATRIZ DE FELIPPE REIS

O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS E SENSÍVEIS DO TRABALHADOR FRENTE ÀS NOVAS TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO

CRICIÚMA
2019

BEATRIZ DE FELIPPE REIS

O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS E SENSÍVEIS DO TRABALHADOR FRENTE ÀS NOVAS TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade do Extremo Sul Catarinense – UNESC, como requisito parcial para a obtenção do Título de Mestre.

Orientador: Prof(ª). Dr(ª). Rodrigo Goldschmidt.

CRICIÚMA

2019

Dados Internacionais de Catalogação na Publicação

R375d Reis, Beatriz De Felippe.
O direito fundamental à proteção de dados pessoais e sensíveis do trabalhador frente às novas tecnologias da informação e comunicação / Beatriz De Felippe Reis. - 2019.
175 p.

Dissertação (Mestrado) - Universidade do Extremo Sul Catarinense, Programa de Pós-Graduação em Direito, Criciúma, 2019.
Orientação: Rodrigo Goldschmidt.

1. Dados pessoais sensíveis. 2. Trabalhadores – Direitos fundamentais. 3. Novas tecnologias. 4. Responsabilidade do empregador. I. Título.

CDD 23. ed. 341.27

Bibliotecária Eliziane de Lucca Alosilla – CRB 14/1101
Biblioteca Central Prof. Eurico Back - UNESC

BEATRIZ DE FELIPPE REIS

"O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS E SENSÍVEIS DO TRABALHADOR FRENTE ÀS NOVAS TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO"

Esta dissertação foi julgada e aprovada para obtenção do Grau de Mestre em Direito no Programa de Pós-Graduação em Direito da Universidade do Extremo Sul Catarinense.

Criciúma, 06 de dezembro de 2019.

BANCA EXAMINADORA

Prof. Dr. Rodrigo Goldschimidt
(Presidente e Orientador(a) – UNESC)

Prof.ª. Dra. Suzéte da Silva Reis
(Membro externo- UNISC)

Prof. Dr. Lucas machado Fagundes
(Membro PPGD/UNESC)

Prof. Dr. Yduan de Oliveira May
(Membro Suplente – Unesc)

Beatriz de Felippe Reis
(Mestrando(a))

Prof. Dr. Reginaldo de Souza Vieira
Coordenador Adjunto do PPGD – UNESC

AGRADECIMENTOS

Várias foram as pessoas que ao longo do mestrado contribuíram para a realização de mais uma etapa na minha formação acadêmica e, por essa razão, não poderia deixar de lhes fazer o devido e merecido agradecimento.

Ao Professor Doutor Rodrigo Goldschmidt, orientador da dissertação, agradeço pelas oportunas correções e sugestões relevantes feitas durante a orientação, as quais muito contribuíram para o meu enriquecimento acadêmico. Acima de tudo, obrigada por estimular o meu interesse pelo conhecimento e pela vida acadêmica.

Aos Professores do Programa de Pós-Graduação em Direito da UNESC, em especial, os Professores Doutores Gustavo Silveira Borges e Ismael Francisco de Souza, que contribuíram com sugestões e materiais para a realização da presente dissertação.

Aos meus colegas de mestrado, em particular à minha colega Vivian Maria Caxambú Graminho, por compartilhar textos e livros imprescindíveis para a realização deste trabalho.

À minha ex-chefe no Tribunal Regional do Trabalho da 4ª Região, Ialdari Maria Benvenutti Santin, por ter acreditado e confiado em mim e ter me autorizado o teletrabalho, tornando possível a realização do Mestrado em Criciúma.

À toda a equipe da Biblioteca José Luiz Ferreira Prunes do Tribunal Regional do Trabalho da 4ª Região, em especial à Magda Rigon Schwarz, a qual nunca mediu esforços, inclusive doando parte do seu tempo, para me ajudar na busca de materiais para a realização desta dissertação.

A todos aqueles que, de uma forma ou de outra, contribuíram para a elaboração do presente trabalho.

Por último, à minha mãe, pelo constante e incondicional apoio e incentivo em todos os objetivos que pretendo alcançar.

“Não é o mais forte que sobrevive, nem o mais inteligente, mas o que melhor se adapta às mudanças.”

Leon C. Megginson

RESUMO

A preocupação em garantir a preservação dos direitos fundamentais da personalidade do trabalhador consiste em uma das principais metas do Direito do Trabalho diante das atuais mudanças disruptivas advindas da chamada quarta revolução industrial. Os dados pessoais e sensíveis, como um direito fundamental do trabalhador brasileiro, merecem especial atenção no ambiente laboral, principalmente em razão do uso intensivo de novas tecnologias por parte do empregador no exercício do poder de controle e de fiscalização. Diante desse cenário, o objetivo principal foi investigar de que forma é possível assegurar uma efetiva proteção aos dados pessoais e sensíveis do trabalhador no contexto da sociedade da informação. Baseado no método dedutivo, por meio da análise da doutrina e da legislação relativas ao tema, a presente dissertação foi estruturado em três partes. A primeira apurou, brevemente, o impacto das novas tecnologias no mundo do trabalho, os limites ao poder diretivo do empregador, especialmente no que tange ao controle eletrônico e, por fim, os riscos reais e potenciais decorrentes do mau uso ou do uso abusivo das tecnologias de informação e armazenamento digital de dados aos direitos fundamentais do trabalhador. A segunda abordou os principais princípios que norteiam o tratamento dos dados e a forma como eles podem ser aplicados nas relações laborais a fim de assegurar aos trabalhadores uma proteção adequada. A terceira e última parte examinou a teoria dos direitos fundamentais como fonte de proteção aos dados pessoais e sensíveis dos trabalhadores, a nova cultura de *compliance* de dados, a responsabilidade das empresas no tratamento dos dados e as políticas e procedimentos previstos na Lei nº 13.709/2018. Constatou-se que, mesmo a legislação trabalhista carecendo de expressa previsão sobre o direito fundamental à proteção dos dados pessoais e sensíveis da pessoa-trabalhadora, é possível assegurar a efetiva proteção e a concretização deste direito na seara laboral a partir das regras gerais existentes no ordenamento jurídico, bem como pelo chamado microssistema jurídico de direitos da personalidade do trabalhador.

Palavras-chave: Dados pessoais e sensíveis. Direitos fundamentais do trabalhador. Novas tecnologias da informação e comunicação. Responsabilidade do empregador.

ABSTRACT

The concern to ensure the preservation of the fundamental rights of the personality of the worker is one of the main goals of Labor Law in the face of the current disruptive changes arising from the so-called fourth industrial revolution. The personal and sensitive data, as a fundamental right of the Brazilian worker, deserve special attention in the work environment, mainly due to the intensive use of new technologies by the employer in the exercise of control and supervision power. However, despite the concern, as the worker is inserted in the business activity and is subordinate to the employer, there will be situations in which their fundamental rights will be restricted. Given this scenario, the main objective was to investigate how it is possible to ensure an effective protection of personal and sensitive data of the worker in the context of the information society. Based on the deductive method, through the analysis of the doctrine and the legislation relating to the subject, this dissertation was structured in three parts. The first, briefly, investigated the impact of new technologies in the world of work, the limits to the employer's governing power, especially with regard to electronic control and, finally, the real and potential risks arising from misuse or improper use of information technologies and digital data storage to the fundamental worker rights. The second addressed the main principles that guide the processing of data and how they can be applied in labor relations in order to ensure workers adequate protection. The third and last part examined the theory of fundamental rights as a source of protection for workers' personal and sensitive data, the new culture of data compliance, the responsibility of companies in the treatment of data and the policies and procedures laid down in Law nº 13.709/2018. It was noted that even the labor legislation lacking express provision about the fundamental right to the protection of personal and sensitive data of the worker, it is possible to ensure the effective protection and implementation of this right in the labor field from the general rules existing in the legal system, as well as by the so-called legal microsystem of rights of the personality of the worker.

Keywords: Personal and sensitive data. Fundamental rights of the worker. New information and communication technologies. Employer Responsibility.

ABREVIATURAS E SIGLAS

AIDS Síndrome da Imunodeficiência Adquirida
AIPD Avaliação de Impacto sobre a Proteção de Dados
APP Aplicativo
ANAMATRA Associação Nacional dos Magistrados da Justiça do Trabalho
ANPD Autoridade Nacional de Proteção de Dados
BRASILCON Instituto Brasileiro de Política e Direito do Consumidor
BYOD Bring Your Own Device
CADE Conselho Administrativo de Defesa Econômica
CDC Código de Defesa do Consumidor
CE Comunidade Europeia
CF Constituição Federal
CJF Conselho da Justiça Federal
CLT Consolidação das Leis do Trabalho
CNDL Confederação Nacional de Dirigentes Lojistas
CONAMAT Congresso Nacional dos Magistrados do Trabalho
DNA Ácido Desoxirribonucleico
DUDH Declaração Universal dos Direitos Humanos
EPD Encarregado da Proteção de Dados
FCPA Foreign Corrupt Practices Act
GDPR General Data Protection Regulation
GPS Global Positioning System
GT29 Grupo de Trabalho de Proteção de Dados do Artigo 29
HIV Vírus da Imunodeficiência Humana
IBGE Instituto Brasileiro de Geografia e Estatística
IDEC Instituto Brasileiro de Defesa do Consumidor
IPEA Instituto de Pesquisa Econômica Aplicada
IRR Incidente de Recurso Repetitivo
ISO International Organization of Standardization
LGPD Lei Geral de Proteção de Dados Pessoais
MDB Movimento Democrático Brasileiro
NTIC Novas Tecnologias da Informação e Comunicação
OCDE Organização para a Cooperação e Desenvolvimento Econômico

OIT Organização Internacional do Trabalho

ONU Organização das Nações Unidas

PEC Proposta de Emenda à Constituição

PET Privacy Enhancing Technology

PIA Privacy Impact Assessment

PIDCP Pacto Internacional dos Direitos Civis e Políticos

PIDESC Pacto Internacional sobre Direitos Econômicos, Sociais e Culturais Humanos

QI Quociente de Inteligência

RFID Radio Frequency Identification

RGPD Regulamento Geral de Proteção de Dados

SDI-I Subseção I Especializada em Dissídios Individuais

TI Tecnologia da Informação

TST Tribunal Superior do Trabalho

UE União Europeia

SUMÁRIO

1 INTRODUÇÃO

Tecnologia e trabalho já fazem parte da nova realidade laboral. Em meio às novas tecnologias da informação e comunicação (NTIC), temas como a privacidade, a proteção de dados, a segurança da informação, os riscos na *internet*, se destacam na chamada sociedade da informação. Tais questões também desafiam o mundo do trabalho, pois as inúmeras ferramentas eletrônicas também trazem consigo o risco maior de lesão aos direitos de personalidade do trabalhador, cada vez mais expostos, dada a maior disponibilidade de informações proporcionada pela rede mundial de computadores.

Além disso, assuntos como o trabalho em plataformas digitais, a robotização, o uso de algoritmos, *big data*, inteligência artificial, meios de vigilância à distância, dentre outros, estão cada vez mais presentes no mundo do trabalho. No tocante às novas formas de organização do trabalho via plataformas digitais, destaca-se que as mudanças disruptivas advindas da revolução digital têm permitido a expansão da chamada economia colaborativa, cujo maior exemplo desta transformação consiste na denominada *uberização* do trabalho.

Com relação à uberização, que ocorre em escala mundial, inúmeras são as preocupações que esse novo fenômeno tem despertado. Uma das maiores inquietações refere-se à disputa entre os trabalhadores para obterem o maior número de tarefas e, com isso, atingirem a maior quantidade de estrelas, aumentando a sua reputação *online*. Contudo, em consequência disso, o que se observa são trabalhadores mais sobrecarregados e mais conectados, resultando em maior número de acidentes de trabalho (inclusive com mortes).

Além disso, há uma ameaça constante aos direitos fundamentais específicos destes profissionais, pois não recebem salários decentes, o tempo de descanso é desrespeitado, as normas de segurança são ignoradas, além da falta formação profissional.

Todavia, os direitos fundamentais inespecíficos dos trabalhadores, ou seja, aqueles que todas as pessoas possuem pela condição de pessoa humana, tais como a privacidade, a proteção de dados pessoais e sensíveis, a reserva da intimidade, são os mais afetados na sociedade da informação, a qual muitas vezes mais se aproxima de uma sociedade de vigilância, em razão do controle praticamente ilimitado propiciado pelas inovações tecnológicas.

Com isso, gradativamente o controle se torna instrusivo e perigoso feito até mesmo à distância, por meio dos algoritmos e da inteligência artifical que recolhem os dados que circulam livremente pelas redes de computadores, deixados voluntária ou involuntariamente, de forma gratuita pelos usuários, e que, em conjunto, permitem ao empresário o conhecimento completo do perfil do trabalhador (abrangendo todo trabalhador ou ex-trabalhador e todo candidato a um emprego), que vai desde aspectos estritamente profissionais a características individuais pertencentes ao âmbito da sua privacidade.

Dessa forma, se por um lado o desenvolvimento tecnológico tem oferecido às pessoas novas ferramentas que as ajudam a alcançar seus objetivos, por outro, elas detém cada vez menos controle sobre os dados que são coletados e sobre as formas como eles são manipulados, acarretando, consequentemente, novos problemas, ameaças e desafios aos seus direitos. Disso decorre a necessidade de proteção da privacidade na vertente da proteção dos dados pessoais e sensíveis.

No campo das relações de trabalho, a situação não é diferente. As NTIC têm permitido que, em nome do interesse empresarial de aprimorar a produção e a tomada de decisões, os empregadores obtenham uma quantidade virtualmente ilimitada de informações sobre os trabalhadores, tornando-se gradativamente mais difícil a separação entre vida privada e vida profissional, a ponto de se falar em uma *nudez tecnológica dos trabalhadores*, na medida em que tecnicamente é possível conhecer quase tudo sobre o trabalhador.

Contudo, observa-se que este acesso cada vez mais abusivo e desproporcional sobre as informações pessoais tem resultado em uma crescente ameaça aos dados pessoais e sensíveis do trabalhador, seja na fase de acesso ao mercado de trabalho, na execução do contrato ou por ocasião da sua cessação. Daí a necessidade de se assegurar uma efetiva proteção a esses dados, na medida em que configuram expressão direta da própria personalidade da pessoa-trabalhadora.

Dessa maneira, nas relações de trabalho, em especial, na relação de emprego, em que há maior grau de subordinação e vulnerabilidade do trabalhador, a necessidade de tutela aos dados pessoais e sensíveis é ainda mais premente, pois, ao adentrar nesses dados, o empregador obtém informações que não revelam somente aptidões profissionais, mas também questões ligadas à privacidade e à intimidade do empregado.

Diante disso, o objetivo central da pesquisa será demonstrar de que forma é possível assegurar uma efetiva proteção aos dados pessoais e sensíveis, como direito fundamental do trabalhador brasileiro, no contexto da sociedade da informação, caracterizada pelo uso intensivo de novas tecnologias.

Destaca-se que, no Brasil, apesar de a Constituição Federal, o Código de Defesa do Consumidor, o Código Civil e o Marco Civil da *internet* protegerem de alguma forma direitos relacionados aos dados e à privacidade, o nível de desenvolvimento tecnológico e a necessidade de se garantir maior segurança jurídica às relações exigia uma legislação que tratasse da proteção dos dados pessoais e sensíveis compatível com a de outros países, sendo que em 2018 foi aprovada pelo Congresso Nacional Brasileiro a Lei nº 13.709/18, conhecida como a Lei Geral de Proteção de Dados Pessoais (LGPD).

Assim, no que tange aos objetivos específicos, o capítulo inicial investigará o impacto das NTIC, em especial no que tange ao tratamento e processamento de dados pessoais e sensíveis dos trabalhadores, enfocando os limites ao poder diretivo do empregador no exercício do controle eletrônico, assim como os principais riscos reais e potenciais do mau uso ou do uso abusivo das tecnologias de informação e armazenamento digital de dados aos direitos fundamentais do trabalhador.

Na sequência, serão definidas as categorias dados pessoais e dados sensíveis como um direito fundamental do trabalhador à luz da doutrina nacional e internacional, utilizando-se, de forma complementar, das recomendações da Organização Internacional do Trabalho (OIT) em matéria de proteção de dados, e do sistema normativo europeu e seus princípios, dada a influência do Regulamento Geral de Proteção de Dados da União Europeia na aprovação da Lei nº 13.709/2018.

O último capítulo, por sua vez, avaliará de que forma as medidas técnicas e organizacionais previstas na Lei nº 13.709/2018, associada à teoria dos direitos fundamentais, bem como a incorporação de programas de *compliance* de dados no âmbito das empresas, podem contribuir para assegurar uma efetiva proteção aos dados pessoais e sensíveis, como direito fundamental do trabalhador. Ainda neste capítulo, será analisada a questão alusiva à responsabilidade do empregador pelos danos causados em razão do exercício de atividade de tratamento de dados pessoais e sensíveis dos trabalhadores, fazendo-se um cotejo entre o que prevê a LGPD e a Consolidação das Leis do Trabalho (CLT).

Além disso, o presente estudo sinalizará que as tecnologias, apesar dos riscos e desafios que acarretam, podem funcionar positivamente na implementação de padrões de boas práticas e da governança, de forma a proteger a privacidade e garantir o direito fundamental dos trabalhadores quanto à proteção dos seus dados.

A pesquisa se justifica pela relevância do tema, o que se confirma na Declaração do Centenário da OIT, aprovada na 108ª Conferência Internacional do Trabalho, a qual, além de colocar o ser humano como o centro das políticas laborais e reconhecer a necessidade de que se estabeleça um piso mínimo de direitos independente da natureza do vínculo de emprego existente, assegura a todos os trabalhadores, independentemente do seu *status*, a garantia da proteção da privacidade e dos dados pessoais.

Ressalta-se ainda que, sobretudo no Brasil, há poucos trabalhos acadêmicos relacionados ao tema da proteção de dados e, se delimitada a pesquisa ao campo do Direito do Trabalho, os estudos encontrados são ainda em menor proporção, conforme consulta realizada junto ao banco de dados da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior.

O trabalho também se justifica, uma vez que, com o uso intensivo das novas ferramentas tecnológicas no ambiente laboral, somada à recente aprovação do regime geral de proteção de dados no Brasil, é natural que discussões judiciais surjam em maior número envolvendo tais questões. Por conseguinte, verifica-se que o tema transcende o espaço acadêmico, atingindo a todos que vivem em sociedade, sendo fundamental fazer avançar as discussões por meio dos diversos canais, em especial, da pesquisa.

Destaca-se, por fim, que dentro da linha de pesquisa Direito, Sociedade e Estado do Programa de Mestrado em Direito da Universidade do Extremo Sul Catarinense, a qual tem por objetivo principal estudar os processos de transformação social que o Brasil e a América Latina vivenciam e que enseja reflexos na constitucionalização dos direitos humanos, insere-se a presente pesquisa, de forma a promover um diálogo permanente e democrático que envolva as instituições estatais e a sociedade.

Portanto, seguindo esta proposta, a presente dissertação vincula-se à linha de pesquisa desenvolvida pelo orientador Prof. Dr. Rodrigo Goldschmidt, líder do Grupo de Pesquisa – DIREITO DO TRABALHO UNESC, o qual tem por objetivo discutir e promover reflexões sobre os principais temas relacionados a políticas

públicas, direitos fundamentais e trabalho digno, com enfoque nas interfaces do direito do trabalho com as novas tecnologias.

Para a execução do presente estudo, o método de abordagem será o dedutivo. Partindo-se da lei geral de proteção de dados pessoais (Lei nº 13.709/2018) e da teoria da eficácia horizontal dos direitos fundamentais, propõe-se a investigar como garantir uma proteção efetiva aos dados pessoais e sensíveis do trabalhador. O método de procedimento será o monográfico, segundo o qual deve-se examinar o tema escolhido, considerando-se todos os fatores e seus aspectos. A técnica de pesquisa será a documental e bibliográfica, pautadas na coleta de dados e pesquisa à jurisprudência, às obras clássicas e contemporâneas, a artigos de revistas jurídicas, a dissertações e teses, a conferências, a documentos oficiais, tais como leis, súmulas e a páginas de *web sites* relacionadas ao tema objeto da pesquisa.

Ao final, por meio desta dissertação, pretende-se demonstrar que, mesmo a legislação trabalhista carecendo de expressa previsão sobre a proteção dos dados pessoais e sensíveis, como um direito fundamental da pessoa-trabalhadora, é possível a concretização deste direito na seara laboral a partir das regras gerais existentes no ordenamento jurídico, bem como pelo chamado *microssistema jurídico de direitos da personalidade do trabalhador*.

2 AS NOVAS TECNOLOGIAS E SEUS REFLEXOS NA RELAÇÃO DE TRABALHO

O avanço tecnológico, somado ao desenvolvimento das chamadas novas tecnologias da informação e comunicação (NTIC), vem impactando profundamente as relações de trabalho, podendo até mesmo se falar em uma nova dimensão do Direito do Trabalho[1], também denominada de Direito do Trabalho 2.0[2], por alguns, ou Direito do Trabalho 4.0[3], por outros.

Hoje, discute-se cada vez mais acerca da indústria 4.0 ou quarta revolução industrial e seus efeitos no futuro do trabalho, especialmente pelo fato de que "a tecnologia de quarta geração é altamente poupadora de mão de obra" (MING, 2017), o que traz sérias consequências, pois reduz o volume de trabalho e os postos de trabalho, podendo ocasionar exclusão social e uma nova onda de pobreza. No mundo digital, a maior parte das empresas não precisam de fábricas, de máquinas para operar ou de estabelecimento físico,[4] mas de informações e dados. "O proprietário dos dados será o empresário, assim como sempre foi o proprietário da fábrica."[5] (SIGNES, 2019, p. 05, tradução nossa).

Outra grande preocupação que as novas tecnologias trouxeram foram os numerosos, complexos e variados problemas jurídicos. Não que as tecnologias sejam

---

[1] Fala-se em uma nova dimensão por conta das mudanças, não só estruturais, mas também funcionais, que alteraram a maneira de efetuar a prestação laboral. Disso decorre "uma mudança capital e um redimensionamento do Direito do trabalho, já não tanto em sentido material de alteração da sua extensão ou volume, mas um processo de revisão do seu âmbito ou extensão, da sua intensidade e do nível que se deve adotar na sua regulamentação." (MOREIRA, 2018, p. 192).

[2] O aditivo 2.0 ao Direito do Trabalho é utilizado por analogia com aquele que designa a chamada Web 2.0, termo popularizado a partir de 2004 pela empresa americana *O'Reilly Media* para designar uma segunda geração de comunidades e serviços, tendo como conceito a "Web enquanto plataforma", envolvendo *wikis*, aplicativos baseados em *folksonomia*, redes sociais, blogs e TI (Tecnologia da Informação). (AGUIAR, 2018, p. 16).

[3] Como explica Moreira (2018, p. 192-193), a evolução do trabalho "começou com o trabalho 1.0., do século XIX e da revolução industrial associado ao surgimento da sociedade industrial, o que originou mudanças no modo de produção e na própria organização do trabalho. Depois temos o trabalho 2.0., do século XX, com o surgimento da produção em massa e advento do Estado Social. Há, depois, o trabalho 3.0, a partir da década de 1970 do século passado, com a globalização e o surgimento do trabalho no computador e a informática; por último tem-se o trabalho 4.0, relacionado com a digitalização, o trabalho em plataformas, a economia colaborativa, o trabalho integrado, que origina uma mudança de valores e de novos compromissos sociais."

[4] São exemplo dessa transformação as empresas que se destacam por serem as maiores dentro de um mercado, sem terem as características até então necessárias para a ele pertencer. É o caso da "Uber como a maior empresa do mundo de transporte, sem ser proprietária de veículos. O Facebook, como maior empresa do mundo de mídia social, sem produzir conteúdo. O AirBnB a maior empresa de aluguéis do mundo, sem possuir imóveis." (AGUIAR, 2018, p. 93).

[5] *Por lo que el propietario de los datos será el empresario igual que lo ha sido siempre el propietario de la fábrica*.

perigosas, pois como refere Moreira (2012, p, 17) “a tecnologia é em si mesma neutra, o mesmo não se podendo dizer do homem que a utiliza.” Tudo irá depender da utilização que lhe é dada, hipótese em que as novas tecnologias podem se tornar especialmente perigosas e apresentarem um quociente de risco.[6]

Partindo desse cenário, os principais objetivos do capítulo consistem em apurar o impacto das novas tecnologias no mundo do trabalho, os limites ao poder diretivo do empregador, especialmente no que tange ao controle eletrônico, a questão dos direitos fundamentais do trabalhador[7] frente às novas tecnologias e, por fim, os riscos reais e potenciais decorrentes do mau uso ou do uso abusivo das tecnologias de informação e armazenamento digital de dados aos direitos fundamentais do trabalhador.

2.1 O IMPACTO DAS NOVAS TECNOLOGIAS NA RELAÇÃO DE TRABALHO

Com o advento da chamada indústria 4.0[8] ou quarta revolução industrial e a globalização, nunca se falou tanto em inteligência artificial, robótica, *internet* das coisas, veículos autônomos, impressão em 3D, nanotecnologia, biotecnologia, ciência dos materiais, armazenamento de energia e computação quântica, dentre outras

---

[6] Com o avanço tecnológico e as potencialidades da análise de megadados, da inteligência artificial e da aprendizagem automática, inúmeros são os riscos e problemas jurídicos advindos. Menciona-se, a título de exemplo, a ampliação da possibilidade de usos secundários dos dados coletados, por meio das tecnologias interativas, o que tem permitido a criação de uma nova ‘mercadoria’, consistente, sobretudo, como aponta Rodotà (2008), na criação de ‘perfis’ individuais, familiares ou de grupos, cedíveis a terceiros. O grande problema é que o uso dessas ferramentas podem ter um impacto significativo nos direitos e nas liberdades das pessoas, inclusive no âmbito das relações laborais, questão esta que será aprofundada no item 2.4.

[7] Para fins da presente pesquisa, adota-se a definição de trabalhador prevista no Repertório de Recomendações práticas da OIT sobre Proteção de Dados Pessoais dos Trabalhadores, segundo o qual “a palavra ‘trabalhador’ designa qualquer trabalhador ou ex-trabalhador e todo candidato a um emprego”. (OIT, 1997, tradução nossa). *La palabra ‘trabajador’ designa a todo trabajador o ex trabajador y a todo candidato a un empleo*.

[8] A indústria 4.0 engloba as principais inovações tecnológicas atinentes à automação, controle e tecnologia da informação, aplicadas aos meios de produção. Baseia-se em processos industriais descentralizados, controlados, autonomamente, por sistemas “cyber-físicos” e pela “internet das coisas”. É precedida pela 1.ª Revolução Industrial (1780-1870), iniciada a partir do surgimento da máquina à vapor; pela 2.ª Revolução Industrial (1870 – 1970), caracterizada pelo uso da energia elétrica, combustíveis derivado do petróleo e o aço; e pela 3.ª Revolução Industrial (1970 – Dias atuais), ocasionada pelo avanço da eletrônica, sistemas computadorizados e pela robótica. O termo “indústria 4.0” surgiu a partir de um projeto do governo alemão que visava o desenvolvimento das tecnologias voltadas para as indústrias, objetivando, sobretudo, aumentar a competitividade, através de “fábricas inteligentes”. (DE AMORIM, 2017).

(SCHWAB, 2016). As novas tecnologias, como *big data analytics*,[9] inteligência artificial, *machine learning*,[10] *cloud computing*,[11] *internet* das coisas (IdC)[12] e manufatura 4.0, são reflexo das transformações do mundo digital, que impactam os padrões de atividade, de interação humana e de produção em ritmo e escala sem precedentes. (IPEA, 2019).

Embora as revoluções industriais do passado tenham produzido efeitos sobre o mundo do trabalho, com a indústria 4.0 a velocidade e o alcance das transformações são significativamente maiores. Se antes as ocupações afetadas pela automatização se concentravam na linha de produção e nas camadas gerenciais intermediárias, agora atividades não rotineiras e altamente especializadas têm sido impactadas pela utilização de algoritmos[13] capazes de decodificar imensas bases de dados e reproduzir padrões complexos. (IPEA, 2019). Tal ocorre porque atualmente

---

[9] "*Big data analytics* refere-se à análise de grandes quantidades de dados gerados por atividades realizadas eletronicamente e por meio de comunicação máquina a máquina." (IPEA, 2019, p. 02).

[10] "*Machine learning* – ou a aprendizagem das máquinas – diz respeito ao desenvolvimento de algoritmos de computador que aprendem autonomamente com base em dados e informações disponíveis." (IPEA, 2019, p. 02).

[11] "*Cloud computing* – ou computação em nuvem – refere-se aos serviços de TICs na internet para acessar servidores, armazenamento, componentes de rede e aplicativos de *software*." (IPEA, 2019, p. 02).

[12] De acordo com o Grupo de Trabalho do artigo 29 para proteção de dados, Parecer nº. 8/2014, de 16 de setembro de 2014, o conceito de Internet das Coisas (IdC) "refere-se a uma infraestrutura em que milhares de milhões de sensores integrados em dispositivos comuns, do dia-a-dia ("coisas", efetivamente, ou coisas ligadas a outros objetos ou indivíduos), são concebidos para registar, tratar, armazenar e transferir dados e, uma vez que estão associados a identificadores únicos, interagir com outros dispositivos ou sistemas que utilizam capacidades de ligação em rede." (COMISSÃO EUROPEIA, 2014, p. 04).

[13] Em sua origem, os algoritmos são sistemas lógicos tão antigos quanto a matemática, os quais ganharam novos propósitos na segunda metade do século passado com o desenvolvimento dos computadores, pois por meio deles, foi possível criar rotinas para as máquinas trabalharem. Um algoritmo corresponde a "uma sequência lógica de passos para resolver um problema, que é escrita em linguagem de programação de computador." Ou seja, "um algoritmo nada mais é do que uma sequência de etapas para resolver um problema ou realizar uma tarefa de forma automática, quer ele tenha apenas uma dezena de linhas de programação ou milhões delas empilhadas em uma espécie de pergaminho virtual." (PIERRO, 2018, p. 19-20). Basicamente são dois os fatores que explicam por que sua aplicação no mundo real vem se multiplicando e se tornando a base do desenvolvimento de *softwares* complexos: o primeiro foi a ampliação da capacidade de processamento dos computadores, que aceleraram a velocidade da execução de tarefas complexas; o segundo foi o advento do *Big Data*, o barateamento da coleta e do armazenamento de quantidades gigantescas de informações, que deram aos algoritmos a possibilidade de identificar padrões imperceptíveis ao olhar humano em atividades de todo tipo. Como exemplo, indica-se alguns casos em que os algoritmos estão presentes: realizada pesquisa no *Google*, a importância de uma página é definida por um algoritmo, que se baseia na quantidade e na boa procedência de *links* que remetem a ela; na engenharia automotiva, no caso dos carros autônomos, são um conjunto de algoritmos que irão processar as informações captadas por câmeras e sensores, tomando instantaneamente as decisões ao volante sem intervenção humana; os algoritmos também estão presentes na procura de atalhos no trânsito via aplicativos de celular. (PIERRO, 2018).

as máquinas são capazes de realizar tanto tarefas rotineiras e repetitivas quanto as que envolvem habilidades cognitivas mais elaboradas.

Em consequência, a disseminação da automação e da robótica, dentro da indústria 4.0, é cada vez mais visível no mundo do trabalho:[14] atividades que antes eram desempenhadas por trabalhadores, hoje estão sendo substituídas por máquinas, computadores, aplicativos de celular, inteligência artificial, entre outros. As transformações advindas da atual revolução tecnológica impõem a necessidade de ajustes, em particular quanto ao mercado de trabalho, pois grande parte dessas novas tecnologias irá substituir atividades manuais e cognitivas, antes exclusivamente humanas, por soluções automatizadas. (IPEA, 2019).

Em uma época de insegurança laboral – trabalhos temporários, contratos de curta duração, desmantelamento das leis trabalhistas[15] – as novas tecnologias surgem como um elemento a mais de incerteza.[16] Dessa forma, o "modelo de trabalho assalariado que dominou a era industrial – no qual um trabalhador renuncia a um grau de liberdade em troca de determinada proporção de segurança – já não pode ser aplicada na atualidade de maneira genérica." (SUPIOT, 2013, p. 157). É preciso se adaptar às mudanças objetivas nas práticas de trabalho decorrentes das novas tecnologias:

> Muitos pesquisadores contemporâneos concordam que a questão não envolve apenas a condição dos direitos individuais do trabalhador, mas também a criação de condições profissionais que assegurem as pessoas, em longo prazo, suas capacidades e necessidades econômicas de maneira suficiente a lhes permitir tomar iniciativas e arcar com responsabilidades. Os termos chaves nesta perspectiva não são postos de trabalho, subordinação e seguridade social, senão trabalho (entendido em todas as suas formas e não só como trabalho assalariado), habilidades profissionais e segurança econômica. (SUPIOT, 2013, p. 157).

---

[14] Como efeito das transformações, as "novas tecnologias da informação introduziram mudanças profundas no mundo do trabalho. As empresas se reduziram, passaram a se utilizar da externalização (terceirização), do teletrabalho, surgindo também a *teledisponibilidade* e a *telessubordinação*. Observa-se aumento do trabalho autônomo dependente, do trabalho precário e da grande massa dos excluídos do mundo formal de trabalho. A globalização e internacionalização do capital determinaram novas estratégias de reestruturação das empresas e novas modalidades contratuais, com o fim de horários fixos e jornadas rígidas." (MANNRICH, 2017, p. 1289).

[15] Vigente desde 11 de novembro de 2017, a Lei nº 13.467/17, conhecida como a lei da "reforma trabalhista", configura um dos marcos da desarticulação dos direitos fundamentais dos trabalhadores, indo em muitos de seus dispositivos de encontro à Constituição Federal.

[16] Acerca do tema, "O Direito do trabalho tem de adaptar-se a estas constantes mutações, e se a introdução da tecnologia nos processos de produção não constitui novidade para este ramo do Direito, já as TIC proporcionam perspectivas únicas capazes de alterar o quadro clássico em que se inseriu o Direito do trabalho." (MOREIRA, 2018, p. 201).

Conforme relatório apresentado no Fórum Econômico Mundial, em Davos, na Suíça, sobre ‘O Futuro do Trabalho: Emprego, Competências e Estratégias da Força de Trabalho para a Quarta Revolução Industrial’ (WORLD ECONOMIC FORUM, 2016), as mudanças disruptivas[17] que atingem o mercado de trabalho podem conduzir a um impacto líquido de mais de 7,1 milhões de postos de trabalho perdidos entre 2015 e 2020. A redução dos postos e o medo do desemprego em decorrência da substituição do homem pela máquina nunca estiveram tão evidentes como agora.

> O baixo custo de automação, o fato de os robôs não necessitarem de direitos trabalhistas e poderem operar 24 horas por dia, deixa muito competitiva a alternativa de automação *versus* o trabalho humano manual, podendo, assim, eliminar potencialmente muitas vagas de trabalho em um futuro próximo. (IPEA, 2019).

Diante disso, tornam-se cada vez mais frequentes os questionamentos sobre como será o trabalho ao longo de todo o século XXI? Quais empregos irão desaparecer? Quais serão criados? Como serão? Alcançarão todas as pessoas? Trabalharemos mais ou menos? O que será das futuras gerações? Tais preocupações são compreensíveis, pois o trabalho é um componente essencial na vida das pessoas.

A substituição do trabalho humano, em especial o trabalho repetitivo, por equipamentos informatizados e microprocessadores, já ocorre gradativamente. Um dos maiores desafios do futuro do trabalho será enfrentar este novo cenário. Diante de tais mudanças, a Organização Internacional do Trabalho (OIT) elaborou o ‘Relatório da Comissão Global sobre o Futuro do Trabalho 2019’, na qual propõe uma agenda centrada no ser humano.[18]

---

[17] São exemplos de fenômenos disruptivos a cibersegurança, a cibernética, a robótica, a biotecnologia, a nanotecnologia, os algoritmos, a inteligência artificial, a computação em nuvem, a *internet* das coisas e a impressão 3D. (CUESTA, 2017).

[18] Tal agenda consiste em três pilares de ação que, juntos, visam impulsionar o crescimento, a equidade e a sustentabilidade para as gerações atuais e futuras. De forma resumida, o primeiro pilar prega maior investimento nas capacidades das pessoas (mediante o oferecimento de um direito universal à aprendizagem ao longo da vida que lhes permita adquirir, requalificar e melhorar as competências; aumento dos investimentos nas instituições, políticas e estratégias que sustentarão as pessoas através das transições do futuro do trabalho; implemento de uma agenda transformadora e mensurável para a igualdade de gênero; oferecimento de proteção social universal desde o nascimento até a velhice). O segundo pilar consiste em aumentar o investimento nas instituições do trabalho (por meio de uma garantia de trabalho universal; ampliação da soberania do tempo de modo a alcançar um equilíbrio entre trabalho e vida pessoal; representatividade coletiva de trabalhadores e empregadores através do diálogo social como um bem público promovido ativamente por meio de políticas públicas; aproveitamento e gerenciamento da tecnologia para o trabalho decente). O terceiro pilar propõe aumentar o investimento no trabalho decente e sustentável e remodelar as estruturas de incentivos às empresas para abordagens de investimento de longo prazo e explorar indicadores suplementares de desenvolvimento e bem-estar humano. (IPEA, 2019).

A fim de alcançar a agenda proposta, é possível se valer de alguns elementos traçados por Aguiar (2018), para garantir a empregabilidade dos chamados trabalhadores neodigitais. O primeiro elemento é a adaptabilidade ao novo, o que deve acontecer por meio da criação de uma espécie de incubadora digital dentro das empresas, das universidades, com acompanhamento do sindicato profissional.[19] O segundo, é a instituição de uma economia criativa aberta a todos, cujo ingresso se dá por intermédio de novas formas e modelos de atuação, com a preservação dos interesses dos mais vulneráveis. O terceiro elemento consiste em uma visão coletiva, a qual deve ser disruptiva, que atenda, de um lado, os trabalhadores, assegurando-lhes a preservação de direitos trabalhistas, e, de outro, das empresas, por meio do aproveitamento de uma maior destreza e competência profissional. Aguiar (2018, p. 80-81) finaliza propondo a criação de uma espécie de 'plataforma sindical-digital de empregos humanos', a ser administrada pelo sindicato profissional, cuja finalidade será a preparação para manutenção de vida empregatícia no mundo digital do trabalho.

As mudanças advindas da indústria 4.0 requerem o envolvimento dos Estados, das instituições internacionais e entidades supranacionais – como a OIT –, as associações empresariais e as organizações sindicais, a fim de evitar ou minimizar as consequências negativas sobre o futuro do trabalho e a sociedade. O diálogo social tripartite entre governos, organizações sindicais e associações empresariais, no âmbito nacional e internacional, é fundamental para encontrar soluções justas que deem respostas ao processo de mudança que se avizinha, sendo a educação instrumento chave para capacitar empresas e trabalhadores aos efeitos da indústria 4.0:

> Seja qual for o impacto da indústria 4.0 sobre os empregos em termos absolutos (de acordo com os estudos mais catastróficos ou o mais otimistas) parece claro que os trabalhadores (e as empresas) hão de saber como se adaptar às novas coordenadas técnicas e produtivas e para isso a educação é o instrumento chave para evitar perda de posto de trabalho. [...] A necessidade de se adaptar às novas demandas da indústria 4.0 (mas também das que venham) requer, em primeiro lugar, certas qualidades dos trabalhadores; em segundo, uma formação; e, em terceiro, a sua

[19] O objetivo é repassar à classe trabalhadora conhecimentos digitais, a fim de enfrentar as novidades do mundo virtual no mundo do trabalho, de forma que o trabalhador não se torne um analfabeto funcional-digital. (AGUIAR, 2018).

> continuidade ao longo de toda sua vida profissional.[20] (CUESTA, 2017, p. 121-122, tradução nossa).

Com relação ao Brasil, pesquisa realizada pelo Instituto de Pesquisa Econômica Aplicada (Ipea) revela que o mercado de trabalho encontra-se estagnado em relação às transformações da chamada quarta revolução industrial. (IPEA, 2019). Apesar disso, mesmo países periféricos, que contam com menos capital para investir em automação e robótica, serão afetados, porém em menor proporção. Em contrapartida, estima-se que novas profissões mais especializadas, que requeiram interação humana e as inovações ligadas à tecnologia de ponta surgirão, especialmente na área da computação, matemática, arquitetura e engenharia. (IHU UNISINOS, 2018).

Destaca-se que o artigo 7º, inciso XXVII, da Constituição Federal Brasileira prevê a proteção do trabalho humano em face da automação, como forma de proteger o trabalhador contra o desemprego tecnológico. Segundo a doutrina, trata-se de uma norma de eficácia limitada[21], que depende de regulamentação.

Todavia, apesar da omissão normativa, a proteção jurídica diante das inovações tecnológicas, como propõe Cavalcante (2018), pode ser extraída dos princípios da função social da propriedade e da função social do contrato (aspecto principiológico), da negociação coletiva de trabalho como instrumento de proteção jurídica do emprego (aspecto formal) e do direito de informação e de consulta dos representantes dos trabalhadores (aspecto material), sem contar a garantia da dignidade do trabalhador, assim como a adoção de políticas públicas sobre a temática.

Importante frisar que as inovações tecnológicas não devem ser concebidas unicamente como uma ameaça, pois representam mecanismos de otimização do processo produtivo, na medida em que são relevantes para o mundo do trabalho,

> sobretudo pelas inovações que são capazes de introduzir no processo produtivo e na forma de organização do trabalho, e permitem melhorar a obtenção, armazenamento, recuperação, exploração, uso e difusão da

---

[20] *Sea cual fuere el impacto de la Industria 4.0 sobre los empleos en términos absolutos (según se den por ciertos los estúdios más catastrofistas o los más optimistas) parece claro que los trabajadores (y las empresas) han de saber adaptarse a las nuevas coordenadas técnicas y productivas y para ello la educación es el instrumento clave para evitar la pérdida de empleos. [...] La necesidad de adaptación a las nuevas demandas de la industria 4.0 (pero de las siguientes que vengan) precisa, en primer lugar, determinadas cualidades de los trabajadores; en segundo, una formación; y en tercero, la continuidad de la misma a lo largo de toda su vida laboral.*

[21] São aquelas que apresentam aplicabilidade mediata e indireta, pois necessitam de uma norma posterior, infraconstitucional, para que incida totalmente sobre o interesse em questão. (SILVA, 2001).

> informação, sendo que estão a converter-se num factor chave para o desenvolvimento do processo produtivo das empresas. (MOREIRA, 2012, p. 20).

A *internet*[22], sobretudo, impulsionou o desenvolvimento das NTIC[23], as quais trouxeram benefícios inegáveis para a sociedade, ensejando uma verdadeira transformação no comportamento social, no surgimento de novos instrumentos e formas de prestação do trabalho, nos meios de comunicação e de aprendizado.[24]

> Cada revolução tecnológica leva a uma reorganização do sistema socioeconômico no qual a revolução da informação tem sido um fator de suma importância que alterou a maneira como as pessoas adquirem e transferem conhecimento. A comunicação e a linguagem. O próprio uso das TIC não afetou apenas a vida privada, laboral e profissional das pessoas em seu ambiente cotidiano. As tecnologias são ferramentas poderosas que permitem novas formas de comunicação, de aprendizado, de socialização, inclusive de entretenimento, ou seja, é um novo meio de cultura.[25] (SOLÍS, p. 03, tradução nossa).

Assim, o resultado desse desenvolvimento tecnológico também é perceptível no universo laboral, seja pela transformação na estrutura organizacional das empresas (por meio da adoção da tecnologia no processo produtivo, na gestão das empresas, na tomada de decisões, na resolução dos problemas, entre outras

---

[22] A *internet* "está a mudar a própria prática do Direito, constituindo um meio de comunicação muito frequente e cada vez mais utilizado nas relações entre empregadores e trabalhadores e entre estes e os seus clientes ou terceiros na medida em que facilita as comunicações ao poupar tempo e custos. Ela confere um acesso cada vez mais rápido e fiável a um número cada vez maior de informação e, no domínio económico, apresenta-se como uma ferramenta importante de informação e de gestão, oferecendo às empresas um enorme número de serviços interactivos." (MOREIRA, 2012, p. 22).

[23] As novas tecnologias da informação e comunicação (NTIC), compreendem o conjunto de inovações baseadas na microeletrônica, na informática – *hardware* e *software* – e nas telecomunicações e cuja finalidade é melhorar os mecanismos de armazenamento, recuperação, transmissão e tratamento da informação. De uma perspectiva histórica, a evolução da informática e das NTIC ocorreram em três etapas: a da macroinformática, a da microinformática e a das redes mundiais e da *internet*. O desenvolvimento destas tecnologias teve suas raízes em meados do século passado, especialmente a partir da II Guerra Mundial. Contudo, foi nos anos setenta do século passado que surgiram uma série de inovações que impulsionaram o desenvolvimento das tecnologias de informação e comunicação, dando ensejo à chamada "micro-eletrônica-digital", até chegar na *internet*, instrumento chave, que provocou uma verdadeira revolução nas comunicações. (MOREIRA, 2010).

[24] Outro aspecto positivo é que "tal como nas revoluções anteriores, várias das possibilidades existentes melhoram a vida das pessoas e permitem a integração no mercado de trabalho de pessoas que tradicionalmente estavam ou poderiam estar excluídas como pessoas portadoras de deficiência, com problemas de mobilidade ou residentes em locais remotos." (MOREIRA, 2018, p. 194).

[25] *Cada revolución tecnológica conlleva a una reorganización del sistema socioeconómico en que la revolución de la información ha sido un factor de suma importancia que ha alterado la manera em como las personas adquieren y hacen transferencia del conocimiento. La comunicación y el lenguaje. El uso mismo de las TIC no solo ha afectado a la vida privada, laboral y profesional de las personas en su entorno cotidiano. Las tecnologías son poderosas herramientas que admiten nuevas formas de comunicación, de aprendizaje de socialización, incluso de divertimento, es decir es um nuevo medio de cultura.*

possibilidades), seja na própria configuração das relações de trabalho (trabalho em plataformas digitais, utilização da prática de BYOD[26] nas empresas, teletrabalho, trabalho à distância, entre outras modalidades).

Acrescenta-se que as novas tecnologias trazem consigo maior independência, flexibilidade e responsabilidade ao trabalhador no desempenho da prestação do trabalho, desencadeando uma proliferação de fenômenos, os quais o Direito do Trabalho precisa enfrentar. Nesse sentido, basta ver o alastramento da chamada "uberização"[27] e da *gig economy*[28] nos últimos anos. A expansão do trabalho sob demanda, conhecido como *work-on-demand* via *apps*[29], tem despertado preocupação, na medida em que, se de um lado cria novas oportunidades de ocupação, de outro, não assegura o acesso a direitos trabalhistas e sociais. Assim, o Direito do Trabalho enfrenta o desafio de enquadrar estas prestações em sua órbita, na medida em que:

> Tanto o trabalho sob demanda quanto via *app* acabam gerando o nascimento de uma nova subclasse social (o crescimento da economia colaborativa

---

[26] Sigla para o termo em inglês *Bring Your Own Device* ou "traga seu próprio dispositivo". Trata-se de "uma prática bastante simples que se explica apenas pelo fato do empresário permitir, sugerir ou obrigar que o empregado utilize seus próprios equipamentos (como *notebooks*, telefones pessoais, *tablets* etc.) para a realização de suas atividades laborais. (GOULART, 2014, p. 72).

[27] A "uberização" das relações laborais refere-se a um "fenômeno que descreve a emergência de um novo padrão de organização do trabalho a partir dos avanços da tecnologia. [...] A partir da segunda década do século XXI, assistimos ao surgimento de um fenômeno novo, a "*uberização*", que, muito embora ainda se encontre em nichos específicos do mercado, tem potencial de se generalizar para todos os setores da atividade econômica." A *Uber* "empresta seu nome ao fenômeno por se tratar do arquétipo desse atual modelo, firmado na tentativa de autonomização dos contratos de trabalho e na utilização de inovações disruptivas nas formas de produção." (OITAVEN; CARELLI; CASAGRANDE, 2018, p. 127-128).

[28] A economia *gig*, também conhecida como "economia do bico", compreende, em linhas gerais, duas principais formas de trabalho: o *crowdwork* e o trabalho *on-demand* por meio de aplicativos. Em síntese, "o 'crowdwork' refere-se a atividades que envolvem a realização de tarefas por meio de plataformas online que colocam em contato diversas organizações e indivíduos com outras organizações e indivíduos por meio da internet, permitindo a aproximação entre consumidores e trabalhadores de todo o mundo. [...] A plataforma de 'crowdwork' mais conhecida é o Amazon Mechanical Turk (MTurk), que oferta a execução de 'tarefas de inteligência humana'." Já o trabalho *on-demand "*se relaciona com a execução de atividades laborais tradicionais, como transporte e limpeza, além de tarefas administrativas e de escritório. Os serviços são oferecidos por meio de aplicativo, que estabelece e garante um padrão de qualidade mínimo na realização do trabalho, bem como seleciona e gerencia a mão de obra. Por meio do uso do aplicativo, o prestador de serviço e o consumidor identificam oferta e demanda, o trabalho é executado em face de uma necessidade apresentada e é feito o pagamento após a finalização do trabalho. [...] O aplicativo de trabalho 'on-demand' mais conhecido é o da Uber, que atua no setor de transportes, no qual um cliente solicita um carro para fazer uma viagem e o motorista, que estiver próximo ao local e disponível, aceita o trabalho." (OITAVEN; CARELLI; CASAGRANDE, 2018, p. 14-17).

[29] *Apps* é uma palavra da língua inglesa e corresponde à redução de *application*, aplicativo. Trata-se de um "programa informático que visa facilitar a realização de uma tarefa num computador ou num dispositivo móvel". (APP, 2019).

> também pode ser visto como uma expansão da precariedade laboral e da transferência de risco para os trabalhadores), o “precário” colaborativo ou tecnológico, isto é, e-precário, (no fundo, "legiões de escravos do clique", "escravos das galeras digitais" – *digital galley slaves* –): pessoas que obtêm a maior parte de sua renda realizando serviços de forma esporádica, dependendo da chamada do cliente, da multidão de clientes, sem horário algum ou renda mínima a ser recebida, sem pausas, sem proteção social, sujeitos ao escrutínio e avaliação de todo o mundo para continuar obtendo remuneração (quem precisa de vigilância e controle se as redes sociais decidem o valor do trabalho) e sem sequer merecer a denominação de trabalhadores. Em muita destas formas, como já indicado, faz-se referência aos trabalhadores como contratados independentes (*independent contractors),* "associados" (*associates*), "gerenciador de tarefas" (*taskers*), "colaboradores" (*partners*) ou outra terminologia que desfoca (torna invisível) sua situação laboral.[30] (CUESTA, 2017, p. 103-104, tradução nossa).

Portanto, a forte influência digital, que impulsiona a explosão de aplicativos com os mais diversos serviços (médico, eletricista, cuidador, manicure, transporte, montador de móveis, entre outros), somada à redução de empregos formais, tem resultado no crescimento e na consolidação do trabalho prestado via plataformas digitais em vários países como uma nova modalidade de organização.

Frente ao atual cenário, o progresso e o avanço tecnológico são inevitáveis. A revolução tecnológica e produtiva gradativamente se consolidam. Torna-se inútil tentar barrar tal avanço, assim como projetar quais serão as profissões do futuro.[31] Logo, o foco passa a ser a formação de trabalhadores com conhecimentos mais amplos e multifuncionais, que atendam às necessidades atuais e futuras, e a minoração dos efeitos em relação aos trabalhadores que ficarão de fora da produção

---

[30] *Tanto el trabajo on demand como vía app acaban generando el nacimiento de una nueva subclase social (el crecimiento de la economía colaborativa puede ser visto también como una expansión de la precariedade laboral y la transferencia del riesgo a los trabajadores), el "precariado" colaborativo o tecnológico, es decir, e-precariado, (en el fondo, “legiones de esclavos del click", "esclavos de la galeras digitales" – digital galley slaves –): personas que obtienen la mayor parte de sus ingresos realizando prestaciones de servicios de forma esporádica, dependiendo de la llamada del cliente, del multitud de clientes, sin horario alguno ni ingreso mínimo a percibir, sin descansos, sin protección social, sometidos ai escrutínio y valoración del mundo entero para continuar obteniendo retribución (quién necesita vigilancia y control si deciden las redes sociales la valía del trabajo) y sin ni siquiera merecer la denominación de trabajadores. En muchas de estas formas, como ya se ha indicado, se hace referencia a los trabajadores como contratistas independientes (independent contractors), "asociados" (associates), "encargados de la tarea" (taskers), "colaboradores" (partners) u otra terminología que desdibuja (invisibiliza) su situación laboral.*

[31] “Independentemente, porém, das incertezas ainda existentes diante de um cenário de grandes e rápidas transformações, alguns aspectos do futuro do trabalho já parecem ser consensuais. O trabalho que envolve força física, classificação e separação de objetos, controle de estoques e operação de máquinas tende a perder importância, sobretudo nos países em que os salários sejam relativamente mais elevados. Por sua vez, habilidades cognitivas, como as que envolvem o raciocínio e o domínio de linguagens, habilidades interpessoais, como o cuidado e o contato humano, habilidades gerenciais e habilidades ligadas às ciências, tanto as da natureza quanto as sociais ou aplicadas, terão maior importância no futuro.” (IPEA, 2019).

da riqueza, especialmente aqueles socialmente mais fragilizados, como os trabalhadores de idade avançada, os jovens sem experiência e os trabalhadores que carecem de formação.

Como forma de assegurar uma proteção a estes trabalhadores, ainda que mínima, debate-se sobre a implantação de uma renda básica universal. Sobre o tema, dada a necessidade de as autoridades públicas fazerem algo para corrigir os desequilíbrios que estão ocorrendo no local de trabalho com a entrada da indústria 4.0, a incorporação da robótica, da inteligência artificial e da *gig economy*, Benítez (2019) acena que:

> Atualmente, considerar a implantação de uma renda básica universal parece uma ideia maluca, porém se assistirmos a vários condicionantes como, por exemplo, a mobilidade internacional de pessoas, os índices de pobreza inclusive em número crescente dentre trabalhadores ativos, a ascensão da indústria 4.0 e da robótica, a abordagem pode ser diferente em face de um iminente futuro incerto no mundo do trabalho.[32] (BENÍTEZ, 2019, p. 01, tradução nossa).

Trata-se de fornecer um suporte de vida, um mínimo de segurança econômica comum aos cidadãos, de forma a garantir a sua liberdade e igualdade. Nessa perspectiva, Cuesta (2017) observa que se uma pessoa não conta com recursos materiais mínimos, o seu direito à liberdade será fictício. Uma segunda justificativa do direito a um mínimo vital é o princípio da igualdade, que deve ser entendido não somente como uma proibição de discriminação (igualdade formal), mas também como assegurador de condições reais de existência (igualdade material).[33]

Assim, a renda básica universal teria por objetivo minimizar as desigualdades promovidas pela revolução tecnológica, garantindo uma assistência às pessoas com pouca ou nenhuma cobertura social, de modo que possam viver com

---

[32] *En la actualidad plantearse la implantación de una renta básica universal parece una idea descabellada, pero si atendemos a varios condicionantes como, por ejemplo, la movilidad internacional de las personas, los índices de pobreza incluso en un número creciente de trabajadores en activo, o el auge de la Industria 4.0 y de la robótica, el planteamiento puede ser distinto de cara a un inminente futuro incierto en el mundo del trabajo*.

[33] Tal prestação também encontra amparo legal na Declaração Universal dos Direitos Humanos, que prevê em seu artigo 25.1 que "Todo ser humano tem direito a um padrão de vida capaz de assegurar-lhe, e a sua família, saúde e bem-estar, inclusive alimentação, vestuário, habitação, cuidados médicos e os serviços sociais indispensáveis" (DUDH, 1948), e no Pacto Internacional sobre Direitos Econômicos, Sociais e Culturais Humanos, que em seu artigo 11.1 dispõe que "Os Estados-partes no presente Pacto reconhecem o direito de toda pessoa a um nível de vida adequado para si próprio e sua família, inclusive à alimentação, vestimenta e moradia adequadas, assim como a uma melhoria contínua de suas condições de vida." (PIDESC, 1966).

dignidade e satisfazer suas necessidades mais essenciais, sem cair em situação de pobreza ou de exclusão social. Há quem sustente que esta renda deve ser compreendida como um direito do cidadão, e não uma concessão do Estado Social, devendo ser concedida sem nenhuma condição, como idade, sexo, riqueza ou padrão de vida.[34] Tal questão é controvertida e ainda despertará muita discussão, dado o avanço das tecnologias e das mudanças no mercado de trabalho pela incidência das transformações digitais.

Por fim, as NTIC, além promoverem uma mudança no processo produtivo, elas também vêm conferindo às empresas o poder de exercer o chamado controle eletrônico com reflexos sobre a vida profissional e privada do trabalhador, tema do tópico seguinte.

2.2 PODER DIRETIVO E LIMITES AO CONTROLE ELETRÔNICO DO EMPREGADOR

Antes de ingressar no chamado controle eletrônico do empregador e seus limites, necessário se faz examinar a figura do empregador e seus poderes, bem como suas implicações nas relações de trabalho. O termo empregador, na sua conceituação jurídica, pode ser extraído a partir do artigo 2º da Consolidação das Leis do Trabalho (CLT), o qual considera “empregador a empresa, individual ou coletiva, que, assumindo os riscos da atividade econômica, admite, assalaria e dirige a prestação pessoal de serviço.” (BRASIL, Decreto-lei nº 5.452, de 1º de maio de 1943). Nas palavras de Nascimento (2011, p. 668):

---

[34] Segundo seus defensores, a renda mínima favoreceria a igualdade entre mulheres e homens, aumentaria o poder de barganha dos trabalhadores, erradicaria a pobreza e diversos problemas associados à indústria 4.0 e à inteligência artificial. Em contrapartida, o seu maior obstáculo seria o seu financiamento (custo contábil). Há, ainda, o receio de que a concessão da renda mínima desincentive o trabalho. (CUESTA, 2017). Vale mencionar que a Finlândia de forma pioneira criou uma espécie de programa piloto de renda mínima universal, no período de janeiro de 2017 a dezembro de 2018, no qual o país pagou 560 euros por mês a 2 mil finlandeses desempregados, selecionados aleatoriamente. O objetivo do plano era avaliar se garantir uma rede de proteção social ajudaria as pessoas a procurar emprego e a apoiá-las se tivessem que trabalhar na chamada *gig economy* (baseada em trabalhadores temporários e sem vínculo empregatício). Como resultado, embora os níveis de emprego não tenham melhorado, os participantes do programa disseram que estavam mais felizes e menos estressados. Há também esquemas semelhantes sendo testados em outros países. Adultos de um vilarejo no oeste do Quênia vão receber US$ 22 por mês até 2028, enquanto o governo italiano está adotando uma "renda cidadã". A cidade de Utrecht, na Holanda, também está realizando um experimento de renda mínima chamado *Weten Wat Werkt* ("Saber o que funciona", em tradução livre) até outubro. (NAGESH, 2019).

> será empregador todo ente para quem uma pessoa física prestar, com pessoalidade, serviços continuados, subordinados e assalariados. É por meio da figura do empregado que se chegará à do empregador, independentemente da estrutura jurídica que tiver.

Exposto o conceito legal de empregador, passa-se ao estudo dos poderes que lhe são juridicamente atribuídos. Segundo Barros (2016, p. 385), a palavra poder, etimologicamente, "deriva do latim vulgar *potere*, da raiz *poti*, que significa chefe de um grupo. O termo 'poder' gira em torno da ideia de posse, de força, de vontade, de obediência e de influência."

O poder empregatício (ou poder intraempresarial, também denominado por parte da doutrina como poder diretivo) é um dos principais efeitos do contrato de trabalho. Consiste em "um conjunto de prerrogativas colocadas à disposição do empregador para direcionamento concreto e efetivo da prestação de serviços pactuada." (DELGADO, 2017, p. 698). Embora a ordem jurídica imponha ao empregador os riscos da atividade empresarial, ela também o confere a "prerrogativa de poder organizar, reger, normatizar, controlar e até punir no âmbito de seu empreendimento." (DELGADO, 2017, p. 727). Importante esclarecer que:

> Na relação de emprego a subordinação é um lado, o poder diretivo é o outro lado da moeda, de modo que, sendo o empregado um trabalhador subordinado, o empregador tem direitos não sobre a sua pessoa mas sobre o modo como a sua atividade é exercida. (NASCIMENTO, 2011, p. 694)

Dessa maneira, partindo da concepção de Nascimento (2011), o poder diretivo manifesta-se em três principais formas: o poder organizativo, o poder de controle sobre o trabalho e o poder disciplinar sobre o empregado. O poder de organização ou poder de comando corresponde:

> ao conjunto de prerrogativas tendencialmente concentradas no empregador dirigidas à organização da estrutura e espaço empresariais internos, inclusive o processo de trabalho adotado no estabelecimento e na empresa, com a especificação e orientação cotidianas no que tange à prestação de serviços. (DELGADO, 2017, p. 751).

Portanto, sendo o empregador o detentor do poder de organização, cabe a ele determinar as normas de caráter técnico às quais o empregado está subordinado. O poder disciplinar, por sua vez, corresponde ao "direito do empregador de exercer a sua autoridade sobre o trabalho de outro, de dirigir a sua atividade, de dar-lhe ordens

de serviço e de impor sanções disciplinares." (NASCIMENTO, 2011, p. 695). Já o poder de controle, objeto do presente estudo:

> dá ao empregador o direito de fiscalizar o trabalho do empregado. A atividade deste, sendo subordinada e mediante direção do empregador, não é exercitada do modo que o empregado pretende, mas daquele que é imposto pelo empregador. (NASCIMENTO, 2011, p. 697).

A doutrina menciona como formas de manifestação do poder de controle a marcação de horários de entrada e saída do trabalho, o controle de portaria, as revistas, o controle das peças produzidas pelo empregado, entre outros. Ocorre que com os avanços tecnológicos, novos mecanismos de controle surgiram e passaram a ser adotados pelas empresas.

As NTIC, especialmente a *internet*, revolucionaram a forma como as pessoas se relacionam. Acerca do tema, Lipovetsky (2007) destaca que um dos traços da chamada hipermodernidade é justamente a hiperconcetividade, resultando em uma crescente exposição do usuário.[35] É como se houvesse quase que uma transparência total, na medida em que as pessoas, ao se conectarem, cedem (in)voluntária um enorme número de informações pessoais na rede mundial[36], permitindo o tratamento e a combinação de dados de caráter pessoal, com consequências para a privacidade[37] das pessoas, em geral, e para a dos trabalhadores, em especial.

Diante disso, o poder de controle do empregador também vem passando por transformações frente à nova realidade, marcada pela revolução tecnológica e pela mutação das formas de organização do trabalho, gerando tensões entre o poder de controle do empregador e os direitos fundamentais dos trabalhadores.[38] Tal poder não é novo nem proibido, tampouco se questiona a sua legitimidade. A grande questão, contudo, está no seus limites frente às novas tecnologias, na medida em que:

---

[35] Com relação a esta mudança comportamental, verifica-se que "as novas tecnologias invadem tudo e geram uma obsessão de interatividade. É preciso estar sempre conectado. Privado e público se confundem. Cada vez mais, cada um quer ser protagonista e contar a sua vida num blog ou noutro mecanismo de exposição o que antes era reservado à família, aos vizinhos e aos amigos." (LIPOVETSKY, 2007, p. XVIII).

[36] Embora as pessoas alimentem cada vez mais os dados que circulam livremente pelas redes de computadores, e, estes tenham cada vez mais efeitos concretos nas nossas vidas, "temos paulatinamente menos controle sobre os dados que são coletados e sobre as formas como eles são manipulados." (BOLZAN DE MORAIS; JACOB NETO, 2018, p. 95).

[37] Apesar das divergências doutrinárias quanto à terminologia de privacidade, adotar-se-á o sentido amplo, qual seja, que inclui vida privada, intimidade e dados pessoais.

[38] Quanto ao tema dos direitos fundamentais, remete-se o leitor ao item 2.3.

> A inovação tecnológica permite e favorece mesmo, através de instrumentos como as videocâmaras, ou a monitorização dos computadores, nas vertentes de controlo dos programas de computadores, de controlo da *world wide web* e de controlo dos *e-mails*, das redes sociais, dos telefones e dos *samrtphones*, de controlo através de *badges*, de *smartcards*, de *chips* incorporados na roupa de trabalho dos trabalhadores, de RFID, de GPS instalados na viatura, de controlo através de dados biométricos, da áudio, vídeo e webvigilância, entre outras formas de controlo, a vigilância da actividade dos trabalhadores contínua e centralizada, transformando assim, por um lado, uma das máximas básicas do *taylorismo* e da direção científica da empresa relacionada com a supervisão e controlo do trabalhador através da observação do comportamento laboral do trabalhador de forma imediata e pessoal. Assim, a transformação operada pelos novos modos de vigilância e controlo origina uma complexa concepção deste poder de controlo do empregador já que este se renova, inclusive dando lugar a novas formas, e chegando a originar, tal como defende PÉREZ DE LOS COBOS ORIHUEL, um "taylorismo de diverso modo", diferente, que aumenta, e muito, este poder de controlo. (MOREIRA, 2018, p. 29-30).

Assim, o surgimento destas novas ferramentas tecnológicas está conduzindo a uma transformação das modalidades de exercício do poder de controle, dando origem ao chamado controle eletrônico do empregador. No anseio de melhor conhecer e controlar tudo o que acontece no âmbito das suas organizações, somada à diminuição de custos, empresas de pequeno, médio e grande porte utilizam-se de forma progressiva dessa nova modalidade. Trata-se de um controle cada vez mais presente e intrusivo, sem limite físico-temporal, que permite ao empregador à distância e em tempo real reunir informações diversas sobre a pessoa do trabalhador, inclusive sobre múltiplas facetas da sua vida, prevendo até mesmo a sua forma de pensar. O acesso é tão amplo e profundo que as empresas conseguem:

> reunir informações sobre os trabalhadores através da observação do que fizeram durante o tempo e no local de trabalho, descobrir os seus interesses e preferências, através da análise dos *sites* mais visitados, possibilitando a criação de perfis dos trabalhadores e a sua seleção baseada nestes dados. Podem, ainda, na fase de selecção, consultar a informação que os candidatos colocam nas redes sociais ou nos seus *blogs* pessoais e excluí-los de acordo com o conteúdo dessa informação. (MOREIRA, 2012, p. 17-18).

Engana-se quem pensa que com as novas modalidades de trabalho (por ex., teletrabalho e *gig economy*), marcadas por uma aparente ausência de subordinação, maior autonomia e flexibilidade, o controle patronal desapareceu. Pelo contrário, com as novas tecnologias, outras formas de controle e de subordinação estão sendo criadas, provocando o surgimento de novos riscos, novas formas de

insegurança no emprego e novas ameaças para os direitos e liberdades dos trabalhadores.

Os novos modelos produtivos que despontam pregam uma disponibilidade quase que perpétua do trabalhador, sendo cada vez mais difícil separar tempo de trabalho e tempo de descanso, vida laboral e vida profissional. Como reação, defende-se o direito à chamada desconexão digital do trabalhador[39], entendido como o direito à vida privada do século XXI. (MOREIRA, 2012).

> Neste *Admirável Mundo Novo do* Trabalho, as mudanças ocorridas na organização e gestão do trabalho conduzem também ao aumento da autonomia organizativa dos trabalhadores que utilizam as novas tecnologias como instrumento de trabalho, dado o carácter predominantemente criativo ou intelectual das suas prestações. Estas, inclusive, inserem-se mais numa ideia de coordenação do que de subordinação, já que o trabalhador não presta a sua actividade, pelo menos na totalidade, dentro do âmbito da organização e direcção de um terceiro, antes a encaminha para a sua própria criatividade, manifestada de forma autónoma e sem exercício aparente de qualquer direcção ou controlo, mas talvez mais controlados do que alguma vez foram. (MOREIRA, 2012, p. 29).

Diante disso, observa-se que o controle exercido, em uma das relações que mais cresce de forma global, a “uberização” do trabalho, torna-se ainda maior em relação ao contratado. Este passa a ser controlado por avaliações de terceiros, surgindo uma nova forma de controle, sendo que, com base nestas avaliações dos usuários-clientes serão tomadas as decisões da empresa proprietária da plataforma, inclusive o próprio desligamento do motorista *uber*.

> O controle exercido pelo contratante através da plataforma ou aplicativo, apesar da distância física, acaba sendo todo abrangente ("quando estão engajados em uma atividade concreta, na maioria dos casos, exercem um controle muito maior sobre esses ‘autônomos’"). O trabalho é observável a todo momento e sem nenhum custo para a empresa, que muitas vezes só remunera dependendo do resultado ou o varia de acordo com o resultado obtido. O sistema utilizado, apesar das infinitas variáveis, é semelhante: através de pontos, estrelas ou outros símbolos, os *crowdworkers* ou autônomos via *app* recebem uma classificação dos clientes. Esta pontuação não obedece a critérios objetivos, mas subjetivos, mas implica conseqüências para o valor do pagamento (ou sua existência), ou para a cessação da atividade. Este sistema coloca os trabalhadores em uma situação de permanente "teste", e impede sua mobilidade entre as plataformas, uma vez

[39] O direito à desconexão digital surgiu como uma resposta frente à diluição dos códigos de espaço e tempo. Visa garantir condições de descanso aos trabalhadores, como também preservar a conciliação da vida pessoal e familiar. Na *gig economy*, tal direito de desconectar poderia consistir em limitar o máximo de conexões, tarefas ou serviços a serem executados em um determinado período de tempo; ou, de outra perspectiva, impedir a desconexão pela empresa mesmo quando a atividade solicitada é rejeitada pelo trabalhador. (CUESTA, 2017, p. 112).

> que a maior recompensa por seu trabalho é obtida por aqueles que são mais bem valorizados por quem encomenda as tarefas. Além disso, às vezes, a plataforma não permite que o prestador de serviços compartilhe sua reputação *online*, em outras, exige exclusividade; na maioria, o próprio sistema o impede."[40] (CUESTA, 2017, p. 112-113, tradução nossa).

Sobre este novo sistema de avaliação, Signes (2018) alerta que com o uso da tecnologia, a forma de controle sobre os trabalhadores vem se transformando, sendo a mais recente a delegação ao cliente da supervisão e controle do trabalhador. Os *smartphones* e os *apps* tornaram mais fácil para o consumidor-cliente da empresa dar sua opinião, não sobre sua satisfação com a empresa, mas especificamente em relação ao desempenho do trabalhador que compareceu ou forneceu o serviço. Trata-se de uma maneira de a empresa obter informações sobre o comportamento do trabalhador a um custo menor. Há situações em que a empresa decide publicar essas avaliações na *internet*: a chamada reputação *online*. Isso implica, por um lado, a possibilidade de o consumidor conhecer a satisfação que os clientes anteriores obtiveram com esse trabalhador em particular. Por outro lado, com a publicação dessas avaliações, o empregado está ciente de que o seu desempenho, julgado insatisfatório por um determinado cliente, será conhecido não só pelo seu empregador, mas também pelos demais clientes e potenciais empregadores.

Contudo, os sistemas reputacionais apresentam uma série de desvantagens, pois, como em qualquer avaliação, respondem a uma experiência pessoal que é avaliada a partir de parâmetros subjetivos, que não podem ser extrapolados para outra pessoa. Além disso, aumentam os riscos psicológicos para os trabalhadores que se sentem observados e julgados por outros cidadãos em todos os momentos. Há, também, o risco derivado do poder que é concedido aos clientes

---

[40] *El control ejercido por el contratante a través de la plataforma o aplicación, pese a la distancia física, acaba por ser omnicomprensivo ("cuando se atienen a una actividad concreta, en la mayoría de casos, ejercen un control mucho mayor sobre estos 'autónomos'"). El trabajo es observable en todo momento y sin coste alguno para la empresa, que muchas veces solo retribuye en función del resultado o varía la misma según el obtenido. El sistema utilizado, pese a las infinitas variables, resulta semejante: a través de puntos, estrellas u otros símbolos, los crowdworkers o autónomos vía app obtienen calificación por parte de los clientes. Dicha puntuación no obedece desde luego a criterios objetivos, sino subjetivos, pero conlleva consecuencias para la cuantía del pago (o su existencia), o para el cese en la actividad. Este sistema coloca a los trabajadores en una situación de permanente "prueba", e impide su movilidad entre plataformas, dado que la mayor recompensa por su trabajo la obtiene quien esté mejor valorado por quienes encargan las tareas. Es más, en ocasiones la plataforma no permite al prestador de servicios compartir su reputación on line, en otras, le exige exclusividad; en la mayoría, el propio sistema lo impide.*

em relação a outros seres humanos, permitindo que eles, os clientes, sejam valorizados sem a devida preparação ou treinamento para exercer esse poder.

Ressalta-se que a vigilância constante e total que os novos meios de controle proporcionam tem contribuído para aumentar a 'dimensão desumana do poder de controlo'[41], com riscos para a saúde dos trabalhadores, tanto físicos, como psíquicos, por saber ou sentir-se constantemente vigiados, podendo provocar uma grande pressão psicológica,[42] conduzindo a casos de assédio moral e doenças como depressão e *stress*. (MOREIRA, 2012).

O novo modelo de trabalho promovido pela revolução tecnológica vem desencadeando um processo de adoecimento dos trabalhadores[43], que se veem bombardeados pela pressão para o atingimento de metas cada vez maiores, por uma desvalorização sua e do seu trabalho, pela grande concorrência para menos trabalho,

---

[41] Cuesta (2017, p. 114) acrescenta que "a ausência de designação como trabalhadores (e pessoas), juntamente com este sistema de pontuação, pode levar à desumanização dos empregadores (os clientes só percebem um número ou variável alfanumérica a qual avaliam). Acabam sendo 'trabalhadores invisíveis', exercendo uma atividade desumanizada em 'fábricas virtuais'. (tradução nossa). *La ausencia de denominación como trabajadores (y personas), unido a este sistema de puntuación, puede conllevar la deshumanización de estos empleadores (los clientes solo perciben un número o variable alfanumérica al que valoran). Acaban siendo "trabajadores invisibles", ejerciendo una actividad deshumanizada en "fábricas virtuales".*

[42] Somado a isso, a "vigilância ostensiva, mesmo sobre atividades lícitas, acarreta efeitos inibitórios sobre a disposição do sujeito para se engajar em atividades criativas, para se expressar livremente, para se associar, para viver as suas crenças mais arraigadas e para participar do processo político." (BRANCO, 2014, p. 337).

[43] Esta é uma das constatações reportadas no Relatório de Riscos Globais 2019 (elaborado pelo Fórum Econômico Mundial), que apresenta os principais riscos a nível macro para 2019 e para a próxima década. De acordo com pesquisas apresentadas no Relatório, "50% dos trabalhadores americanos dizem estar 'frequentemente ou sempre exaustos devido ao trabalho', um aumento de quase um terço em 20 anos. Em outro estudo, trabalhadores do Reino Unido, quando convidados a identificar as principais causas do stress no local de trabalho, metade citou a pressão de tempo e demandas irrealistas. O mesmo estudo assinalou a preocupação dos trabalhadores com a falta de consulta sobre as mudanças no local de trabalho (31%) e a falta de controle sobre o trabalho que realizam (27%). A automação tem sido uma fonte de perturbação no local de trabalho. Ela permitiu que um grande número de funcionários subisse na cadeia de valor e escapasse de tarefas monótonas e perigosas, mas já em 1959 a Organização Mundial da Saúde vinha notando impactos psicológicos adversos não apenas da automação, mas até mesmo da perspectiva de automação. Pesquisa publicada em 2018 sugere que, nos Estados Unidos, um aumento de 10% na probabilidade de ser afetado pela automação está associado a reduções na saúde física e mental de 0,8% e 0,6%, respectivamente. (WORLD ECONOMIC FORUM, 2019, p. 39-40, tradução nossa). *According to one study, 50% of American workers say they are "often or always exhausted due to work", up by almost a third in 20 years. In another study, when UK workers were asked to identify the main workplace causes of stress, half cited unrealistic time pressure and demands. The same study noted employees' concern about lack of consultation on workplace changes (31%) and lack of control over the work they do (27%). Automation has long been a source of disruption in the workplace. It has allowed huge numbers of employees to move up the value chain and escape monotonous and dangerous tasks, but as far back as 1959 the World Health Organization was noting adverse psychological impacts not just of automation but even of the prospect of automation. Research published in 2018 suggests that, in the United States, a 10% increase in the likelihood of being affected by automation is associated with decreases in physical and mental health of 0.8% and 0.6%, respectively*.

pela pouca criatividade e capacidade de controle, pela falta de perspectiva de um futuro estável e pelo consumo de remédios tarja preta, em razão da ansiedade, da depressão e da perda de sentido do trabalho. Dessa forma, se as NTIC, por um lado facilitam o trabalho humano, por outro, comprometem a saúde do trabalhador e representam fator de risco laboral.

Não é por que alguém é empregado de uma empresa que seus direitos, especialmente os relacionados a sua personalidade (ligados à dignidade da pessoa do trabalhador)[44] serão absolutamente anulados. O empregador, no exercício do poder diretivo, não pode fazer uso intensivo das ferramentas tecnológicas de forma a eliminar completamente a privacidade, a intimidade, a proteção aos dados do trabalhador, até porque, "com o advento destas inovações tecnológicas, é fundamental que os trabalhadores possam usufruir dos mesmos direitos que tinham anteriormente." (MOREIRA, 2012, p. 32). Afinal, na relação de trabalho, o que é colocado à disposição do empregador é a força de trabalho do trabalhador, e não a sua pessoa.

Assim, o aumento do poder de controle reacendeu o clássico debate entre o equilíbrio dos direitos e liberdades fundamentais do trabalhador e o legítimo direito do empregador de dirigir e controlar as tarefas daqueles, pois caso tal controle não seja usado com cautela, pode conduzir "ao parcial desaparecimento de alguns direitos fundamentais no âmbito da empresa, como o da privacidade, liberdade e dignidade dos trabalhadores." (MOREIRA, 2012, p. 31).

> As novas formas de controlo tornaram-se também automáticas, não estando os supervisores limitados pelo que podem ver mas pela quantidade de dados e de aspectos que conseguem recolher através do controlo exercido pelas máquinas. O controlo torna toda a realidade transparente, provocando a visibilidade do que até aí era ignorado ou invisível. O "olho electrónico" torna-se omnipresente e mecânico, conduzindo a sensações de controlo total que podem alterar os sentimentos dos trabalhadores e provocar o seu medo pelo facto de não estar confinado espacialmente ao local de trabalho, podendo estender-se para outros locais, inclusive sítios muito íntimos, e por não ter barreiras temporais. (MOREIRA, 2012, p. 31).

[44] Acerca do tema, Goldschmidt (2019b) defende a existência de um microssistema jurídico de direitos da personalidade do trabalhador (tais como a honra, a imagem, a intimidade, a liberdade de ação, a autoestima, a sexualidade, a saúde, o lazer e a integridade física, que podem ser extraídos do rol exemplificativo do artigo 223-C da CLT), o qual deve ser observado no âmbito das relações de trabalho, a fim de proteger e promover a dignidade da pessoa humana (base sobre a qual se assentam os direitos da personalidade, nomeadamente, do trabalhador).

Surge, portanto, a necessidade de se definir limites a este controle eletrônico, de modo a compatibilizá-lo com a proteção dos direitos fundamentais de quem presta o trabalho. A Constituição Federal de 1988 rejeita "condutas fiscalizatórias e de controle da prestação de serviços que agridam à liberdade e dignidade básicas da pessoa física do trabalhador." (DELGADO, 2017, p. 754). Nesse sentido, a liberdade pessoal dos trabalhadores e os seus direitos da personalidade configuram limites a este poder[45], não se admitindo que, em nome do direito de propriedade, da segurança, da produtividade, o direito relativo às liberdades individuais seja exterminado pelas novas tecnologias. Não se trata de defender:

> um retrocesso em matéria de evolução de empresas, pois elas têm de ser competitivas e essa competitividade passa necessariamente pela informatização e por adquirir cada vez mais NTIC, que têm inúmeros aspectos positivos. Mas, se é inquestionável que as empresas devem ser eficientes, dinâmicas, e actualizadas, não é menos certo que esses objectivos não podem ser conseguidos à custa da dignidade dos trabalhadores, à custa de direitos fundamentais que tão duramente foram conquistados. As empresas devem pensar o trabalho e a sua organização em função da pessoa humana e não o inverso, [...]. (MOREIRA, 2012, p. 39).

Nessa mesma linha, Goldschmidt (2019b, p. 31) assevera que:

> [...] os direitos da personalidade estão disciplinados em várias esferas normativas, em especial no marco dos tratados internacionais, na Constituição Federal e nas normas infraconstitucionais, a exemplo do Código Civil e Consolidação das Leis do Trabalho.
> É possível constatar que o homem e sua dignidade assumiram a centralidade de todos esses níveis normativos sistêmicos. Em face disso, observou-se uma evolução do direito para reconhecer que o SER é mais importante do que o TER. Viu-se, então, que o direito deslocou o seu centro de gravidade, dando prevalência sobre os direitos da personalidade sobre os direitos patrimoniais, reconhecendo a dignidade humana como o bem maior a ser protegido e promovido, sendo que os bens patrimoniais, a riqueza, a economia em si, devem servir ao homem e ao seu pleno desenvolvimento, e não o contrário.

Portanto, é preciso lembrar que o trabalhador é um sujeito e não um objeto, de forma que as ferramentas tecnológicas é que devem adaptar-se, e não o contrário,

---

[45] Sobre o tema, Delgado (2017, p. 726) aduz que "Os direitos de personalidade são imantados de tutela jurídica significativa, de inegável potência e efetividade, não só por derivarem diretamente da Constituição da República, como também por serem instrumento imprescindível de realização do sentido mais notável dos princípios constitucionais da centralidade da pessoa humana na ordem jurídica e da dignidade da pessoa humana, além do próprio sentido lógico e teleológico do conceito de Estado Democrático de Direito, todos claramente afirmados pelo Texto Máximo Republicano. Nessa medida estabelecem claro contraponto ao poder empregatício, em qualquer de suas dimensões — poder normativo, diretivo, fiscalizatório e poder disciplinar."

sob pena de haver quebra da confiança mútua que deve permear as relações de trabalho. A solução, portanto, faz-se por meio da harmonização das dimensões jurídicas contrapostas, ou seja:

> por meio da atenuação, racionalização e civilização do poder empregatício, que tem de passar a se harmonizar à relevância dos princípios, regras e institutos constitucionais que asseguram tutela aos direitos de personalidade do ser humano partícipe da relação de emprego no polo obreiro. (DELGADO, 2017, p. 727).

Acerca do tema, menciona-se o julgado da 6ª Turma do Tribunal Superior do Trabalho (TST) que condenou a companhia aérea *American Airlines* ao pagamento de danos morais por submeter uma empregada ao “detector de mentira” (polígrafo). No caso em tela, a companhia realizava uma a duas vezes por ano questionamentos como: "Você já cometeu crimes ou já foi presa?"; "Vende ou já vendeu narcóticos?"; "Tem antecedentes de desonestidade?"; "Cometeu violações de trânsito?"; "Deve dinheiro para alguém? Quem? Quanto?", "Já roubou qualquer propriedade do local onde trabalha?"; "Desde seu último teste, já usou drogas ilegais?"; "Intencionalmente já permitiu que alguém viajasse com documentos falsos?"; "Permitiu que alguém violasse os procedimentos de segurança?"; e "Já permitiu contrabando em alguma aeronave?". Segundo a companhia aérea, o detector seria uma medida válida para segurança dos passageiros que utilizam a companhia, sujeitos a acidentes e "ataques terroristas". Os ministros do TST entenderam que a atitude da empresa era inconstitucional, pois discriminatória, viola a intimidade dos empregados, causa danos à honra e à imagem, extrapola o exercício do poder da empresa, além do que, o uso do polígrafo não é um mecanismo legalmente previsto no ordenamento jurídico do Brasil. Para o relator, Ministro Maurício Godinho Delgado, o uso do polígrafo assemelha-se aos métodos de investigação de crimes exclusivo da polícia, havendo outros procedimentos legais mais eficazes para a segurança da companhia aérea. (TST, 2010).

Como se observa, apesar de as tecnologias contribuírem para o desenvolvimento, elas também podem ser usadas de forma a lesar direitos

fundamentais dos trabalhadores, sobretudo a sua dignidade e a privacidade[46]. Diante disso:

> A tentativa de encontrar um justo equilíbrio entre os poderes do empregador e os direitos e liberdades fundamentais dos trabalhadores constitui o objecto do *Novo Direito do trabalho*. "O direito do trabalho está a mudar de paradigma: de um direito dos trabalhadores passa-se para um direito dos direitos da pessoa no trabalho", sendo que a dignidade do Homem impõe-se sobre quaisquer outras considerações. (MOREIRA, 2018, p. 33).

Destaca-se ainda que um dos problemas na utilização das NTIC é que o empregador pode se valer delas "para finalidades nem sempre legítimas, disfarçadas com *biombos linguísticos* sob a forma de interesses produtivos ou comerciais, quando na realidade pode ser de controlo puro e duro que se trate." (MOREIRA, 2012, p. 18).

Assim, muito tem se discutido até que ponto a vida privada do trabalhador pode ser objeto de investigação por parte das empresas com vistas ao controle, ou seja, com que finalidade determinado dado sobre o trabalhador é coletado, e de que forma é possível estabelecer um limite do invasivo quando o empregador extrapola e adentra na privacidade e intimidade do trabalhador.

Percebe-se que com as novas tecnologias, as empresas, com o objetivo de facilitar a seleção para a contratação, formação, controle de qualidade e proteção de bens da empresa, têm ultrapassado o limite da necessidade ao investigar sobre a vida privada do trabalhador. Torna-se gradativamente mais comum a adoção de questionamentos e levantamentos sobre condições de saúde, hábitos cotidianos, lazer, convicções ideológicas, religiosas e políticas, resultando em uma investigação que recai sobre a existência do funcionário para além dos limites da empresa, o que caracteriza um abuso de direito, no caso, do poder empregatício, nos termos do artigo 187 do Código Civil[47].

Verifica-se, portanto, que as transformações contemporâneas dessa forma de poder introduzem dispositivos de controle que adentram em dimensões da

---

[46] A respeito da privacidade, Doneda (2000, p. 13) atenta para o fato de ela ser um elemento da personalidade, cuja "cotidiana redefinição de forças e meios que possibilitam a intromissão na esfera privada dos indivíduos demanda uma tutela de caráter incessantemente mutável", concluindo que a única tutela eficaz é a dinâmica e integral.

[47] "Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes." (BRASIL. Lei nº 10.406, de 10 de janeiro de 2002).

existência que anteriormente eram consideradas como privadas, incluindo aí, além da fisiologia, também o psiquismo, a socialização, a afetividade e a imaginação.

Todavia, estas novas ferramentas digitais e formas de controle produzem novas formas de exclusão social que são ainda mais radicais, na medida em que, como mencionado, permitem identificar aspectos relacionados ao estilo de vida que o trabalhador adota quando se encontra fora do seu local de trabalho, rastreando até mesmo aspectos ligados à vida social, sexual, familiar e afetiva, e que será levado em consideração nos processos de seleção, nos programas de ascensão funcional, nas premiações e nos processos de dispensa.

De outra sorte, embora o trabalhador possa resistir e se opor a este exame da vida pessoal, dada a nudez tecnológica[48] a que se encontra exposto, a fragilidade dos contratos de trabalho, o alto índice de desemprego, o medo de perder o trabalho, a dificuldade de conquistar uma promoção, enfim, todo este conjunto de fatores leva o trabalhador a “consentir” com aquilo que a empresa solicita, mesmo que isso implique o tratamento de informações pessoais e, consequente, exposição de questões privadas, que nada avaliam a aptidão profissional em si.

Como visto, apesar do progresso tecnológico no mundo do trabalho, que permitiu ao empregador a implementação de formas sofisticadas de controle e vigilância, é preciso atentar para o fato de que o poder diretivo não é ilimitado. O trabalhador é titular de direitos e garantias, os quais introduzem e cristalizam na relação laboral a incidência de direitos humanos tidos como fundamentais, como ocorre na Constituição Federal de 1988, ponto este que será aprofundando no tópico seguinte.

2.3 OS DIREITOS FUNDAMENTAIS DO TRABALHADOR FRENTE ÀS NOVAS TECNOLOGIAS

As inovações digitais estão mudando a realidade, alterando formas, condições e a própria natureza jurídica dos institutos, produzindo efeitos diretos sobre garantias jurídicas fundamentais. Tais mudanças implicam situações novas que o

[48] Com relação à nudez tecnológica, Moreira (2018, p. 197) ressalta que sem dúvida ela “está presente com um controlo cada vez mais intrusivo feito por máquinas e um novo tipo de prova denominada de prova digital ou prova virtual, já que o essencial do controlo é invisível ao olho humano e toda uma vida profissional e pessoal está associada a uma máquina.”

Direito precisa regular, especialmente no que tange à proteção dos direitos fundamentais dos trabalhadores frente às novas tecnologias. Como referido, a indústria 4.0 pressupõe uma transformação digital que envolve as empresas e seus trabalhadores.

> Nos últimos vinte anos, os especialistas em Direito do Trabalho têm se preocupado sobre a forma como as novas tecnologias de informação e comunicação (TIC) afetam os postos de trabalho. Dezenas de estudos têm surgido, motivados pela redução da privacidade dos trabalhadores – monitoramento dos computadores, câmeras, GPS, redes sociais – pelo aumento da carga de trabalho fora da jornada – teletrabalho, *e-mails* – etc. Todas essas preocupações se devem, principalmente, ao aumento do poder de vigilância e controle do empregador sobre o trabalhador. Entretanto, nos últimos dois anos, parece que as novas tecnologias estão afetando os trabalhadores de outra maneira: fazendo com que desapareçam. (SIGNES, 2017, p. 28).

Com as novas tecnologias e a redução de custos das transações, as empresas não necessitam mais possuir grandes estruturas organizacionais, logo, descentralizam seu processo produtivo e criam redes de produção dispersas. Tal mudança contribui para o surgimento de um modelo de trabalho que está se espalhando para mais e mais empresas: trata-se do chamado *ghost work* ou trabalho fantasma, por meio do qual "a indústria de inteligência artificial funciona com o trabalho invisível de humanos trabalhando em condições isoladas e muitas vezes terríveis", dando a impressão de que "não há humanos envolvidos nesse ciclo, que é apenas uma questão de software trabalhando sua mágica."[49] (HAO, 2019). Essa é apenas uma das inúmeras novas questões para qual o Direito do Trabalho precisa atentar.

[49] Acerca do tema, o jornal britânico *The Guardian* publicou um artigo sobre o trabalho fantasma e a questão da invisibilidade dos trabalhadores. Nele, o jornal revela a realidade da produção do *Google Assistant*, mostrando que "por trás da 'mágica' de sua capacidade de interpretar 26 idiomas está uma enorme equipe de linguistas, trabalhando como subcontratantes, que devem rotular os dados de treinamento para que isso funcione. Eles ganham baixos salários e são rotineiramente forçados a trabalhar horas extras não pagas. Suas preocupações com as condições de trabalho foram repetidamente descartadas." O caso não é isolado, "É apenas uma história entre dezenas que começaram a abrir as cortinas de como funciona a indústria de inteligência artificial. Trabalhadores humanos não apenas rotulam os dados que fazem a IA funcionar. Às vezes, os trabalhadores humanos são a inteligência artificial. Por trás da IA de moderação de conteúdo do Facebook existem milhares de moderadores de conteúdo; atrás da Amazon Alexa é uma equipe global de transcritores; e por trás do Google Duplex, às vezes, as pessoas muito humanas chamam a AI que imita os seres humanos. A inteligência artificial não funciona com poeira mágica. Ela é executada em trabalhadores invisíveis que treinam algoritmos implacavelmente até que eles automatizem seus próprios trabalhos." (HAO, 2019).

Partindo disso, o ponto que aqui interessa, e, que muitas vezes tem passado desapercebido, diz respeito aos direitos fundamentais dos trabalhadores neodigitais. Com relação ao tema, Moreira (2018, p. 196) assinala que:

> Ocorrem, ainda, novas ameaças para os direitos fundamentais dos trabalhadores, quer os direitos fundamentais *específicos,* com a prática de baixos salários principalmente para as tarefas que exigem menos qualificação, pagos à peça ou tarefa, a falta de respeito pelos tempos de trabalho com a crescente intensificação do mesmo e a cultura da urgência, o não respeito pelos direitos coletivos, ou o aumento dos riscos para a segurança e saúde dos trabalhadores quer físicos, quer psicológicos, quer para os direitos fundamentais *inespecificos,* como a privacidade, já que se está perante uma intensificação do controlo eletrónico, panótico[50], automático, ainda mais intrusivo para a privacidade pois é implementado por algoritmos, falando-se de um "trabalhador algoritmo" ou, em inglês de um *algocracy,* podendo correr-se o risco até de uma coisificação da pessoa humana.[51]

Portanto, observa-se que os direitos fundamentais dos trabalhadores correm sério risco, seja pela falta de proteção social e a crescente precarização das relações laborais,[52] que não lhes asseguram uma vida digna, seja porque o controle

---

[50] O Panóptico ou *pan-óptico* foi idealizado em 1785 pelo filósofo e jurista inglês Jeremy Bentham. Corresponde a um edifício em forma de anel, no meio do qual há um pátio com uma torre no centro, que permite a um único vigilante observar todos os prisioneiros, sem que estes possam saber se estão ou não sendo observados, sendo que é justamente isso que faz com que os prisioneiros adotem o comportamento desejado pelo vigilante. O panóptico é aplicável não só às prisões, mas também aos manicômios, às escolas, às fábricas, dentre outras. Trata-se de uma categoria adotada por Michel Foucault, em sua obra 'Vigiar e Punir', para tratar da sociedade disciplinar. (POMBO, 2019).

[51] Acerca da coisificação, "se alguém é reconhecido como *sujeito*, não pode ser simultaneamente tratado como se fosse *objeto*, *coisa*." O Tribunal Constitucional alemão, para verificar eventual violação da dignidade em torno da proibição de a pessoa ser coisificada, adota o critério designado de "fórmula do objecto". A fórmula combina dois fatores complementares: parte de uma "determinação *negativa* do conteúdo normativo do princípio constitucional da dignidade da pessoa humana", ou seja, centra-se no apuramento da violação da dignidade, e, ao invés "de se orientar para a definição e a extração das consequências normativas do que significa ser *sujeito*, ser *pessoa*, constrói a *norma* da dignidade em torno da exclusão do tratamento como *objeto*, como *coisa*, como *meio*." Assim, a "dignidade humana não estará a ser respeitada quando, num processo de intencional ou de negligente *coisificação*, a pessoa deixe de ser considerada como sujeito autónomo e fim em si e seja degradada à condição de algo fungível, tão só instrumento ou simples meio de realização de fins alheios." (NOVAIS, 2016, p. 112-114). Em igual sentido, a Declaração de Filadélfia, que consiste na Constituição da OIT, é explícita ao afirmar dentre os seus princípios fundamentais que "o trabalho não é uma mercadoria", não permitindo a coisificação da pessoa humana e a dissociação do trabalhador da prestação de trabalho. (OIT, 1944).

[52] O trabalho "não significa apenas a principal fonte de rendimento para a maior parte das pessoas no mundo. O trabalho é também uma forma de estar em sociedade e de dignidade e até de identidade, sendo a forma de participação na sociedade para muitos. O emprego tem de ser visto como uma atividade que visa a produção material de bens e serviços úteis à sociedade e não como atividade apenas para permitir uma acumulação de riqueza. O trabalho não deve ser visto apenas como uma forma de remuneração económica mas também como uma forma de estar em sociedade. E a carência de emprego ou a sua existência precária minam as possibilidades de integração, podendo romper-se a coesão social e criarem-se situações de exclusão, fazendo perigar a estabilidade social da sociedade." (MOREIRA, 2018, p. 200).

total direto e à distância, espacial e temporal, e a exigência de uma conexão constante, vem transformando estes trabalhadores em autênticos escravos digitais,[53] dificultando a separação entre as fronteiras da vida pessoal e da vida profissional.

Com relação ao primeiro aspecto (relacionado aos direitos fundamentais específicos dos trabalhadores[54]), uma das razões básicas de proteção é a desigualdade de poder de negociação e a falta de uma verdadeira autonomia da vontade ao acertar as condições de trabalho. O fato de os "novos trabalhadores" terem características diferentes dos trabalhadores do século XIX não lhes retira a necessidade de similar proteção. Embora o trabalhador na revolução industrial não pudesse negociar suas condições contratuais livremente frente ao poder capitalista, hoje em dia, a situação é a mesma. "Os prestadores pessoais de serviços da Amazon MTurk não podem negociar suas condições para formar parte da plataforma, [...]. O mesmo ocorre com o restante das plataformas." (SIGNES, 2017, p. 36). Com relação a este ponto, cabem as seguintes reflexões:

> Quando nestas plataformas se esquece uma das máximas que originou o surgimento do Direito do trabalho como ramo do Direito autónomo e que é a de que o trabalho não é separável da pessoa que o presta, e que não existe trabalho mas só existem as pessoas que trabalham, não estaremos a retornar aos inícios da revolução industrial? O trabalho prestado é mercantilizado com base no pagamento da tarefa à peça, com retribuições extremamente baixas que nem cumprem os limiares mínimos relacionados com um trabalho decente, onde não há direito à segurança social, ou a assistência na doença, com eventual trabalho infantil, em que os trabalhadores são sujeitos a discriminação, e sem qualquer respeito por direitos coletivos, assim como sem respeito pelos direitos fundamentais, não estaremos a retornar ao passado? (MOREIRA, 2018, p. 197).

As mudanças introduzidas com a evolução tecnológica não acabam com as inseguranças a que os trabalhadores estão sujeitos, sejam os antigos ou os

---

[53] Em sua obra 'O Privilégio da Servidão: o novo proletariado dos serviços na era digital', o sociólogo Ricardo Antunes enxerga a automação como uma maior precarização do trabalho humano e menciona o caso do esquema "zero hora", nascido na Inglaterra, o qual vem ganhando espaço no mundo. Trata-se de uma espécie de trabalho sem contrato, no qual não há previsibilidade de horas a cumprir nem direitos assegurados. Quando há demanda, basta uma chamada e os trabalhadores e as trabalhadoras devem estar on-line para atender o trabalho intermitente. As corporações se aproveitam: expande-se a "uberização", ampliasse a "pejotização", florescendo uma nova modalidade de trabalho: o *escravo digital*. Tudo isso para disfarçar o assalariamento. (ANTUNES, 2018).

[54] "Os direitos fundamentais específicos dos trabalhadores (direitos fundamentais sociais) são aqueles direitos expressamente destinados aos trabalhadores e que têm, em regra, como sujeito passivo os empregadores, públicos ou privados. Como exemplo, pode ser citado a quase totalidade dos direitos fundamentais previstos no art. 7º da CF de 1988 (limitação da jornada de trabalho, férias acrescidas de 1/3, proteção contra a despedida arbitrária ou sem justa causa, décimo terceiro salário), cuja aplicação nas relações privadas sequer é questionada." (VECCHI, 2011, p. 119).

novos[55], os quais continuam expostos à flexibilização de direitos, aos baixos salários[56] (sem garantia de um valor fixo ou invariável) e à transferência de riscos do empreendimento[57]. Daí porque a necessidade de incidência de normas mínimas de proteção para reestabelecer o desequilíbrio de poderes, sob pena destes trabalhadores ficarem desamparados, sem a segurança de um nível mínimo de subsistência, com reflexos sobre um dos direitos mais fundamentais: o da existência condigna.[58] Partindo disso:

> [...] economicamente, os "microempresários" e os trabalhadores tradicionais pertencem à mesma realidade e requerem também proteção legislativa frente ao desequilíbrio existente entre as partes. Por essa razão, pode não ter muito sentido debater se os trabalhadores do século XXI, juridicamente, se encaixam ou não na definição de contrato de trabalho do século XIX, mas sim que a verdadeira questão futura a debater será se a realidade, sobre a qual se discute a proteção oferecida, é a mesma. Com as características vistas em epígrafe se pode constatar uma resposta afirmativa: as necessidades de proteção seguem existindo para os novos trabalhadores, ou como são chamados "microempresários", sejam dependentes ou independentes."[59] (SIGNES, 2017, p. 39).

---

[55] Por vezes, estes trabalhadores também recebem a denominação de parceiros, colaboradores, empreendedores. (OITAVEN; CARELLI; CASAGRANDE, 2018).

[56] Outro ponto sobre os baixos salários é que eles também impedem que exista poder de consumo na sociedade, na medida em que reduzem o poder de compra dos cidadãos e, quando sobra algum excedente, a tendência é poupar para quando faltar. Além disso, os trabalhadores com renda variável tendem a recorrer ao mercado de capital para fazer empréstimo e se deparam com maiores dificuldades no mercado para estabilizar sua renda, pois os mercados de capitais e os seguros são frequentemente fechados para eles. (SIGNES, 2017).

[57] A CLT, no seu artigo 2º, *caput*, coloca sob ônus do empregador os riscos do empreendimento, independentemente do insucesso que possa se abater sobre este. Nesse sentido, a "característica da *assunção dos riscos do empreendimento ou do trabalho* consiste na circunstância de impor a ordem justrabalhista à exclusiva responsabilidade do empregador, em contraponto aos interesses obreiros oriundos do contrato pactuado, os ônus decorrentes de sua atividade empresarial ou até mesmo do contrato empregatício celebrado. Por tal característica, em suma, o empregador assume os riscos da empresa, do estabelecimento e do próprio contrato de trabalho e sua execução. A presente característica é também conhecida pela denominação *alteridade*." (DELGADO, 2017, p. 461-462).

[58] A garantia de uma existência condigna encontra suporte na dimensão prestacional (positiva) do princípio da dignidade da pessoa humana, "segundo a qual o Estado, a comunidade e o particular devem prover os meios com os quais o homem possa viver com dignidade, proporcionando saúde, educação, trabalho, moradia, enfim, todos os bens do mundo da vida necessários para uma existência digna." (GOLDSCHMIDT, 2009b, p. 107). Nesse sentido, "quando se fala de dignidade da pessoa humana na sua dimensão prestacional, o que se "presta" não é a dignidade em si, como se fosse esta um objeto material que pode ser entregue *in natura* a alguém, mas os "meios" com os quais o homem mantém e promove a dignidade que lhe é inata. Vale dizer, "prestacionar" dignidade é proporcionar, de fato e de direito, os meios que dignificam a existência humana, dando-lhe um sentido, uma condição de respeitabilidade." (GOLDSCHMIDT, 2009b, p. 74).

[59] Como forma de proteger estes trabalhadores excluídos pelo novo modelo de negócio, "o objetivo, definitivamente, seria incluir no âmbito de proteção do contrato de trabalho aqueles prestadores de serviços pessoais que, independentemente da forma da prestação do serviço, teriam sua autonomia da vontade diminuída devido a sua frágil posição negocial. Dessa forma, todos aqueles prestadores pessoais de serviços que se encontram diante de um contrato de adesão, com impossibilidade de negociar realmente as condições contratuais na prestação pessoal de serviços, resultariam protegidos pela norma trabalhista." (SIGNES, 2017, p. 42).

Com relação ao segundo aspecto (relacionado aos direitos fundamentais inespecíficos dos trabalhadores[60]), alusivo ao impacto das novas tecnologias e ao controle empresarial que resulta em uma nudez tecnológica[61] quase que total do trabalhador, com reflexos sobre a sua privacidade e intimidade, a questão central consiste em como proteger adequadamente tais direitos fundamentais na era digital. O tema é complexo, por isso, convém analisar, ainda que de forma breve, como os direitos fundamentais se comportam no contexto digital das relações de trabalho.

O termo direitos fundamentais (*droits fondamentaux*) aparece na França, por volta de 1770, no movimento político e cultural que conduziu à Declaração dos Direitos do Homem e do Cidadão de 1789. Vários autores buscaram definir o conceito de direitos fundamentais. Canotilho (2003, p. 393) aduz que "direitos fundamentais são os direitos do homem, jurídico-institucionalmente garantidos e limitados espacio-temporalmente." E, complementa, "seriam os direitos objectivamente vigentes numa ordem jurídica concreta." Para Pérez Luño (2010, p. 33), trata-se dos "direitos humanos positivados nas constituições estatais." Ao traçar uma perspectiva histórica dos direitos naturais do homem aos direitos fundamentais constitucionais, Sarlet (2012, p. 25) refere que:

> Somente a partir do reconhecimento e da consagração dos direitos fundamentais pelas primeiras Constituições é que assume relevo a problemática das assim denominadas "gerações" (ou dimensões) dos direitos fundamentais, visto que umbilicalmente vinculada às transformações geradas pelo reconhecimento de novas necessidades básicas, de modo especial em virtude da evolução do Estado Liberal (Estado formal de Direito) para o moderno Estado de Direito (Estado social e democrático [material] de Direito), bem como pelas mutações decorrentes do processo de industrialização e seus reflexos, pelo impacto tecnológico e científico, pelo processo de descolonialização e tantos outros fatores direta ou indiretamente relevantes neste contexto e que poderiam ser considerados.

Assim, desde que reconhecidos pelas primeiras Constituições, os direitos fundamentais passaram por várias transformações no que tange ao seu conteúdo, a sua titularidade, eficácia e efetivação. A doutrina, em geral, menciona a existência de

---

[60] "Os direitos fundamentais inespecíficos são aqueles direitos não destinados de forma especial aos trabalhadores nas relações de trabalho ou de emprego, mas, sim, os direitos fundamentais que são destinados a qualquer pessoa humana, a qualquer cidadão. Como exemplos, podem ser citados os direitos à intimidade e vida privada, direito de expressão, liberdade religiosa, devido processo legal e direito à honra." (VECCHI, 2011, p. 119).

[61] Quanto ao tema da nudez tecnológica, remete-se o leitor ao item 2.2.

três gerações de direitos[62], contudo, fala-se também na existência de uma quarta, quinta e até mesmo de uma sexta geração, dada a mutação histórica experimentada pelos direitos fundamentais. (SARLET, 2012). Nesse sentido, partindo da análise dos direitos fundamentais sob as diferentes dimensões, há quem considere os direitos fundamentais de terceira dimensão uma resposta à degradação de direitos e liberdades fundamentais, sobretudo pelo uso de novas tecnologias.

> Nesta perspectiva, assumem especial relevância o direito ao meio ambiente e à qualidade de vida (que já foi considerado como direito de terceira geração pela corrente doutrinária que parte do critério da titularidade transindividual), bem como o direito de informática (ou liberdade de informática), cujo reconhecimento é postulado justamente em virtude do controle cada vez maior sobre a liberdade e intimidade individual mediante bancos de dados pessoais, meios de comunicação etc., mas que – em virtude de sua vinculação com os direitos de liberdade (inclusive de expressão e comunicação) e as garantias da intimidade e privacidade suscita certas dúvidas no que tange ao seu enquadramento na terceira dimensão dos direitos fundamentais. [...] Com efeito, cuida-se, no mais das vezes, da reivindicação de novas liberdades fundamentais, cujo reconhecimento se impõe em face dos impactos da sociedade industrial e técnica deste final de

[62] Essencialmente, os direitos fundamentais de primeira dimensão são produto do pensamento liberal-burguês do século XVIII, de cunho individualista, surgindo e afirmando-se como direitos do indivíduo frente ao Estado, mais especificamente como direitos de defesa, demarcando uma zona de não intervenção do Estado. São apresentados como direitos de cunho "negativo", pois dirigidos a uma abstenção, ou seja, "direitos de resistência ou de oposição perante o Estado". Assumem relevo no rol desses direitos, especialmente pela sua notória inspiração jusnaturalista, os direitos à vida, à liberdade, à propriedade e à igualdade perante a lei. São, posteriormente, complementados por um leque de liberdades, incluindo as assim denominadas liberdades de expressão coletiva (liberdades de expressão, imprensa, manifestação, reunião, associação etc.) e pelos direitos de participação política, tais como o direito de voto e a capacidade eleitoral passiva, revelando, de tal sorte, a íntima correlação entre os direitos fundamentais e a democracia. Também o direito de igualdade, entendido como igualdade formal (perante a lei) e algumas garantias processuais (devido processo legal, *habeas corpus*, direito de petição) se enquadram nesta categoria. A doutrina os denomina de direitos civis e políticos. Os direitos fundamentais de segunda dimensão são conhecidos como direitos econômicos, sociais e culturais. Têm como nota distintiva a sua dimensão positiva, pois não visam mais evitar a intervenção do Estado na esfera da liberdade individual. Tais direitos caracterizam-se, ainda hoje, por outorgarem ao indivíduo direitos a prestações sociais estatais, como assistência social, saúde, educação, trabalho etc., revelando uma transição das liberdades formais abstratas para as liberdades materiais concretas. Além disso, distinguem-se dos clássicos direitos de liberdade e igualdade formal, estando relacionados ao princípio da igualdade, entendida esta num sentido material. Para além dos direitos de cunho positivo, englobam as denominadas "liberdades sociais", como a liberdade de sindicalização, do direito de greve, bem como do reconhecimento de direitos fundamentais aos trabalhadores, tais como o direito a férias e ao repouso semanal remunerado, a garantia de um salário mínimo, a limitação da jornada de trabalho, apenas para citar alguns dos mais representativos. Assim como os direitos da primeira dimensão, também os direitos sociais reportam-se à pessoa individual, não se confundindo com os direitos coletivos e/ou difusos da terceira dimensão. Quanto aos direitos fundamentais de terceira dimensão, também chamados de direitos de solidariedade e fraternidade, trazem como nota distintiva o fato de se desprenderem, em princípio, da figura do homem-indivíduo como seu titular, destinando-se à proteção de grupos humanos (família, povo, nação), e caracterizando-se, consequentemente, como direitos de titularidade coletiva ou difusa. A doutrina refere como exemplos de direitos de terceira dimensão os direitos à paz, à autodeterminação dos povos, ao desenvolvimento, ao meio ambiente e qualidade de vida, bem como o direito à conservação e utilização do patrimônio histórico e cultural e o direito de comunicação. (SARLET, 2012).

> século. Na sua essência e pela sua estrutura jurídica de direitos de cunho excludente e negativo, atuando como direitos de caráter preponderantemente defensivo, poderiam enquadrar-se, na verdade, na categoria dos direitos da primeira dimensão, evidenciando assim a permanente atualidade dos direitos de liberdade, ainda que com nova roupagem e adaptados às exigências do homem contemporâneo. (SARLET, 2012, p. 34-35).

Outros, contudo, defendem o direito de informática, incluindo o direito fundamental à privacidade na *internet*, como um direito de quinta dimensão, na qual estão situados "os direitos advindos das tecnologias de informação (Internet), do ciberespaço e da realidade virtual em geral" (WOLKMER, 2002, p. 21), cabendo ao Direito regulamentar as questões relacionadas a este novo universo virtual. Ocorre que, embora o livre acesso à *internet* (baseado na universalidade do acesso à informação) venha se consolidando como um direito humano[63], o que é relevante para a legitimação dos direitos fundamentais no contexto da *internet*, muitos são os problemas envolvendo a privacidade e o resguardo aos dados dos usuários[64], situação que também se verifica nas relações trabalhistas, sendo tal viés o ponto central desta pesquisa.

Voltando ao campo laboral, verifica-se que os direitos e liberdades fundamentais dos trabalhadores também correm perigo em face do uso desenfreado das novas tecnologias, as quais tornam-se potenciais difusoras de ameaças à vida privada e aos dados pessoais e sensíveis do empregado[65], na medida em que

---

[63] A Organização das Nações Unidas (ONU) publicou o Relatório A/HRC/17/27 sobre a promoção e proteção do direito à liberdade de opinião e de expressão, na qual considera que desconectar as pessoas da *internet* configura uma violação dos direitos humanos e vai contra a lei internacional. Segundo a ONU, violar este direito significa violar o artigo 19 da Declaração Universal dos Direitos Humanos e o Pacto Internacional sobre os Direitos Civis e Políticos. (UNITED NATIONS, 2011).

[64] Com relação ao tema, destacam-se dois casos emblemáticos envolvendo problemas de privacidade de dados: as últimas eleições para a presidência dos Estados Unidos e a campanha *Brexit*. A denúncia feita pelos jornais *The New York Times* e *The Guardian* levantou dúvidas sobre a transparência e o compromisso da empresa *Facebook* com a proteção de dados dos seus usuários, na medida em que o *Facebook* permitiu que a empresa americana *Cambridge Analytica* (empresa de análise de dados que trabalhou com o time responsável para campanha do republicano Donald Trump nas eleições de 2016, nos Estados Unidos, e, na Europa, foi contratada pelo grupo que promovia o *Brexit* – a saída do Reino Unido da União Europeia) acessasse informações de mais de 50 milhões de usuários sem o consentimento destes para fazer propaganda política. A empresa teria tido acesso ao volume de dados ao lançar um aplicativo de teste psicológico na rede social. Aqueles usuários do *Facebook* que participaram do teste acabaram por entregar à *Cambridge Analytica* não apenas suas informações, mas os dados referentes a todos os amigos do perfil. Com base nesses dados, a empresa criou um sistema que permitiu predizer e influenciar as escolhas dos eleitores nas urnas. (BBC NEWS Brasil, 2018). Acerca do tema, há o documentário 'Privacidade Hackeada', da *Netflix*, que mostra em detalhes o caso que abalou as estruturas de várias gigantes da tecnologia e o quanto os dados dos usuários estão vulneráveis.

[65] Os dados pessoais correspondem a todo tipo de informação relacionada com um trabalhador identificado ou identificável, ao passo que os dados pessoais sensíveis incluem os relacionados à vida

facilitam o armazenamento e a distribuição das informações, de forma ainda mais impactante e devastadora.[66]

Evidentemente que nenhum direito é absoluto, e que o empregador, no exercício da sua atividade econômica, tem interesse em aperfeiçoar a sua produção. Contudo, não se pode consentir que, em nome do aumento da produtividade e da supremacia dos interesses empresariais[67], direitos fundamentais de personalidade estejam expostos a maior risco de lesão. Nesse sentido:

> [...] dentro do largo espectro de direitos fundamentais, há, pelo menos uma diferenciação a ter em conta quando se considera a relação entre dignidade e direitos fundamentais: se há direitos que, por natureza, estão mais próximos ou mais intimamente associados à dignidade da pessoa humana, esses são os chamados direitos fundamentais de personalidade, ou seja, aqueles, de entre os direitos fundamentais, que respeitam e se fundam na própria existência do seu titular considerado como *persona*, incluindo-se, aí, as garantias fundamentais de protecção da vida, da integridade física e psíquica, da liberdade geral de acção e de uma esfera pessoal reservada. (NOVAIS, 2015, p. 185).[68]

Os direitos fundamentais em apreço também se operam nas relações privadas, podendo ser invocado em face de outro particular (por meio da eficácia

---

sexual da pessoa, a sua condição de afiliado a um sindicato, suas origens raciais, suas opiniões políticas, suas crenças religiosas e antecedentes criminais. (OIT, 1997).

[66] Sobre o tema, menciona-se o chamado direito à autodeterminação informacional, surgido dentro da jurisprudência constitucional germânica, vocacionado para a proteção da personalidade face às novas tecnologias computacionais de recolha, tratamento, acesso exterior e disseminação de dados pessoais, e que garante o controle sobre os dados que lhe dizem respeito e sobre o seu conhecimento e acesso por parte de terceiros. (NOVAIS, 2016).

[67] "Não é nova a prática do empregador de coletar informações sobre experiências e conhecimentos do empregado, suas características física e psicológicas, suas habilidades, adaptabilidade, capacidade de compromisso, desempenho e comportamento em geral. Ela está indissociavelmente ligada ao interesse empresarial de aperfeiçoar tanto a produção quanto o processo de seleção de mão de obra." [...] O que mudou é o fato de que o processamento de quantidade virtualmente ilimitada de informação sobre os empregados passou a ser um componente absolutamente normal da vida de (ou no) trabalho." Com o uso dos computadores e o desenvolvimento das tecnologias da informação, problemas com espaço para armazenamento, acessibilidade e a operacionalidade da informação praticamente desapareceram. Assim, "os dados coletados durante anos permanecem presentes e usáveis e é possível a sua adição e correção, tornando a informação confiável, constantemente disponível e inteiramente utilizável. Uma vez armazenados, os dados podem ser livremente combinados e usados para múltiplas finalidades." (SANDEN, 2014, p. 23-24).

[68] Nesse sentido, "muitos dos direitos fundamentais são direitos de personalidade, mas nem todos os direitos fundamentais são direitos de personalidade." Os direitos de personalidade abarcam "os direitos de estado (por ex: direito de cidadania), os direitos sobre a própria pessoa (direito à vida, à integridade moral e física, à privacidade), os direitos distintivos da personalidade (direito à identidade pessoal, direito à informática) e muitos dos direitos de liberdade (liberdade de expressão). Tradicionalmente, afastavam-se dos direitos de personalidade os direitos fundamentais políticos e os direitos a prestações por não serem atinentes ao ser como pessoa. Contudo, hoje em dia, dada a interdependência entre o estatuto positivo e o estatuto negativo do cidadão, e em face da concepção de um direito geral de personalidade como "direito à pessoa ser e à pessoa devir", cada vez mais os direitos fundamentais tendem a ser direitos de personalidade e vice-versa." (CANOTILHO, 2003, p. 396).

horizontal dos direitos fundamentais), não se resumindo a disciplinar as relações entre indivíduos e os Poderes Públicos.[69] No âmbito das relações laborais a situação não é diferente, sendo campo para a incidência dos direitos fundamentais.

Como visto, com as NTIC multiplicam-se as controvérsias envolvendo novas formas de controle por meios tecnológicos (vigilância por câmeras ou por drones, geolocalização, registro de dados biométricos, implantação de *microchips* em trabalhadores, análise maciça de dados – *Big Data* e etc.), revelando males que resultam da perda da privacidade, da intimidade e da proteção aos dados.

Diante disso, um dos questionamentos que surge é como conciliar o princípio da liberdade de gestão empresarial e organização dos meios de trabalho que visem à promoção da produtividade e desenvolvimento da empresa com os direitos fundamentais da reserva da intimidade da vida privada e da proteção de dados pessoais e sensíveis do trabalhador na era digital? Embora este não seja o problema da presente pesquisa, tal questão tem despertado preocupação por parte da doutrina trabalhista.

É inegável que o exercício do direito de direção (em especial, o poder de controle) por parte do empregador, que resulta dos direitos de propriedade e de livre-iniciativa, apresenta potencial atrito com os direitos fundamentais dos trabalhadores. Neste caso, o direito de propriedade do empregador *versus* o direito à intimidade, à vida privada, à proteção de dados e à dignidade da pessoa humana do trabalhador, devem ser analisados à luz do princípio da proporcionalidade.[70]

Portanto, não é possível dizer que os fins justificam os meios, ou seja, o empregador, no exercício do poder diretivo, não está autorizado a fazer uso intensivo das ferramentas tecnológicas de forma a anular os direitos fundamentais de

---

[69] Acerca do tema, Silva (2011, p. 52-53) esclarece que "[...] não é somente o Estado que pode ameaçar os direitos fundamentais dos cidadãos, mas também outros cidadãos, nas relações horizontais entre si." E complementa que não apenas no caso da relação de indivíduos com as grandes corporações, mas também todas as relações entre particulares, em qualquer relação entre si, mas especialmente naquelas em que ocorre uma posição de desigualdade entre as partes, estão vinculadas aos direitos fundamentais.

[70] Segundo Barroso (2010), o princípio da proporcionalidade é utilizado com frequência, como instrumento de ponderação entre valores constitucionais contrapostos, aí incluídas as colisões de direitos fundamentais e as colisões entre estes e interesses coletivos. Nesse sentido, a privacidade, como direito humano e fundamental, em que pese sua inalienabilidade e irrenunciabilidade, não é um direito absoluto. Na análise do caso concreto, tal princípio pode ser restringido. Essa mitigação, contudo, exigirá um juízo de ponderação a ser exercido em consonância com o princípio da proporcionalidade, ou seja, o sacrifício da privacidade deve justificar-se em prol de um bem maior, não havendo outro meio adequado a se atingir o resultado necessário.

personalidade do trabalhador que, apesar de não serem absolutos, eventual limitação deve observar a duração, o alcance, a intensidade e a finalidade.[71]

Por fim, as tecnologias de informação e de armazenamento trazem ao empregador uma gama de informações sobre os trabalhadores, as quais antes ele não tinha acesso, permitindo que o tratamento e a combinação de dados de caráter pessoal seja cada vez mais frequente. O problema é que tal prática permite revelar informações sobre pessoas específicas, podendo ensejar riscos reais e potenciais aos direitos fundamentais dos seus titulares, tema do tópico seguinte.

2.4 RISCOS REAIS E POTENCIAIS DO MAU USO OU DO USO ABUSIVO DAS TECNOLOGIAS DE INFORMAÇÃO E ARMAZENAMENTO DIGITAL DE DADOS AOS DIREITOS FUNDAMENTAIS DO TRABALHADOR

A economia baseada em dados ganha força dentro da quarta revolução industrial. Trata-se de uma profunda mudança no mundo global, na qual os tradicionais insumos de produção estão sendo substituídos por uma produção intensiva em dados, alterando as bases concorrenciais do mercado, podendo elevar os níveis de produtividade de 5% a 10%.[72] Estima-se que o mundo alcançará a marca de mais de 30 bilhões de dispositivos conectados à *internet* em 2020 e que o impacto da *internet* das coisas nos diversos setores econômicos pode chegar a US$ 11,1 trilhões em 2025, o que corresponderia a 11% da economia global. (IPEA, 2019).

---

[71] Para maior aprofundamento no tema, remete-se à leitura da Dissertação de DACHERI, Emanueli. **O impacto da tecnologia nas relações de trabalho**: uma análise à luz da teoria da eficácia horizontal dos direitos fundamentais da personalidade dos trabalhadores. 2019. Dissertação (Mestrado em Direito) – Universidade do Extremo Sul Catarinense, 2019.

[72] A produção e o armazenamento de dados alcança tamanha proporção que, "adaptando-se a este novo panorama de big data, a economia, cada vez mais voltada para a informação, passou a aproveitá-lo: coletando e tratando estes dados, tidos como insumos, novos modelos de negócio surgiram. Os dados se tornaram tão valorizados que já chegaram a dizer se tratar do 'novo petróleo'. [...] Em tempos de crise econômica, como a que experiencia o planeta desde a bolha imobiliária norte-americana de 2008, negócios baseados em dados surgem como uma atraente alternativa: é um insumo, como se viu, que se produz em escalas imensas diariamente, e cujo acesso, coleta e armazenamento torna-se mais barato quanto mais evoluem as tecnologias para tanto. Serviços aparentemente gratuitos são, de igual maneira, atraentes para os usuários e consumidores em tempos de depressão econômica. Serviços online como o Facebook, WhatsApp, Twitter, Instagram e Snapchat, entre vários outros que monetizam os dados pessoais, são de acesso 'gratuito'; muitos aplicativos para smartfones e tablets também o são – desde que, em troca da utilização deles, o usuário ceda seus dados pessoais. Não à toa, tais companhias, apesar da crise, têm apresentado consistente crescimento econômico. O lucro do Facebook, em 2016, foi de 10 bilhões de dólares. Em 2017, a receita do Google foi de 24,75 bilhões de dólares." (CARVALHO; GUIMARÃES; OLIVEIRA, 2017).

Assim, a chamada era datacêntrica ou dataísmo[73] ganha espaço no século XXI. Os inúmeros dados livres presentes nas redes sociais, nas teses acadêmicas,

[73] Dataísmo é a expressão empregada por Harari (2016, p. 369) em sua obra “Homo Deus: uma breve história do amanhã” para se referir à religião que vem emergindo, a qual “não venera nem deuses nem o homem – venera dados”, e que no século XXI pode “afastar os humanos, mudando de uma visão antropocêntrica para uma visão datacêntrica.” (HARARI, 2016, p. 392). O “dataísmo inverte a pirâmide tradicional do aprendizado. Até então, os dados eram considerados apenas o primeiro passo na longa cadeia de atividade intelectual. Supunha-se que os humanos refinassem dados em informação, informação em conhecimento e conhecimento em sabedoria. Os dataístas, contudo, acreditam que os humanos não são mais capazes de lidar com os enormes fluxos de dados, ou seja, não conseguem mais refiná-los para obter informação, muito menos para obter conhecimento ou sabedoria. O trabalho de processamento de dados deveria, portanto, ser confiado a algoritmos eletrônicos, cuja capacidade excede muito a do cérebro humano.” (HARARI, 2016, p. 371). Aprofundando a questão do dataísmo, o “supremo valor dessa nova religião é o “fluxo de informação”. Se vida é informação em movimento, e se achamos que a vida é boa, deveríamos estender, aprofundar e disseminar o fluxo de informação no Universo. Segundo o dataísmo, as experiências humanas não são sagradas, e o *Homo sapiens* não é o ápice da criação ou o precursor de algum futuro *Homo deus*. Humanos são apenas instrumentos para a criação da internet de todas as coisas que eventualmente poderá se estender para fora do planeta Terra para cobrir a galáxia e até mesmo o Universo. Esse sistema de processamento de dados cósmico seria como Deus. Estaria em toda parte e controlaria tudo, e os humanos estão destinados a se fundir dentro dele. [...] O dataísmo não se limita a profecias ociosas. Como toda religião, tem seus mandamentos práticos. Primeiro e preliminarmente, um dataísta tem de maximizar o fluxo de dados conectando-se cada vez a mais mídias, produzindo e consumindo mais e mais informação. Como outras religiões bem-sucedidas, o dataísmo também é missionário. Seu segundo mandamento é conectar tudo ao sistema, inclusive hereges que não querem ser conectados. E “tudo” quer dizer mais do que humanos. Quer dizer tudo quanto é *coisa.* Meu corpo, é claro, mas também os carros na rua, as geladeiras na cozinha, as galinhas em suas gaiolas e as árvores na floresta — tudo deveria se conectar à internet de todas as coisas. A geladeira vai monitorar o número de ovos na gaveta e informar a galinha na gaiola quando uma nova entrega for necessária. Os carros vão conversar uns com os outros, e as árvores na floresta vão informar sobre o clima e os níveis de dióxido de carbono. Não podemos deixar nenhuma parte do Universo desconectada da grande rede da vida. Inversamente, o maior dos pecados é bloquear o fluxo de dados. O que é a morte senão uma situação na qual as informações não fluem? Por isso o dataísmo sustenta que a liberdade de informação é o maior bem de todos. Raramente alguém consegue aparecer com um valor completamente novo. A última vez que isso aconteceu foi no século XVIII, quando a revolução humanista pregou os estimulantes ideais de liberdade, igualdade e fraternidade humanas. A partir de 1789, a despeito de numerosas guerras e levantes, os humanos ainda não conseguiram aparecer com nenhum valor novo. Todos os conflitos e lutas subsequentes foram travados ou em nome dos três valores humanistas, ou em nome de valores ainda mais antigos, como o de obedecer a Deus ou o de servir à nação. O dataísmo é o primeiro movimento desde 1789 a criar um valor realmente inovador: o da liberdade de informação.” (HARARI, 2016, p. 383-385). Por fim, “agora a religião dos dados diz que cada palavra e ação suas são parte de um grande fluxo de dados, que algoritmos o vigiam constantemente e se importam com tudo o que você faz e sente. A maioria das pessoas gosta muito disso. Para os verdadeiros crentes, estar desconectado do fluxo de dados acarreta o risco de perder o próprio sentido da vida. De que adianta fazer ou experimentar qualquer coisa se ninguém souber disso, e se isso não contribuir para a troca global de informações? De acordo com o humanismo, as experiências ocorrem dentro de nós e devemos encontrar em nosso interior o significado de tudo o que acontece, impregnando desse modo o Universo de significado. Os dataístas acreditam que experiências não têm valor se não forem compartilhadas e que não precisamos — na verdade *não podemos* — encontrar significado em nosso interior. Só precisamos gravar e conectar nossa experiência ao grande fluxo de dados, e os algoritmos vão descobrir seu significado e nos dizer o que fazer. Vinte anos atrás, turistas japoneses eram motivo de riso universal porque levavam consigo câmeras e tiravam fotos de tudo o que estava à vista. Hoje todos fazem isso. Se você for à Índia e deparar com um elefante, você não vai olhar para o animal e se perguntar “O que estou sentindo?” — você estará ocupado demais pegando seu *smartphone*, tirando uma foto do elefante, postando-a no Facebook, e depois conferindo sua conta a cada dois minutos para ver quantas curtidas obteve. [...] O novo lema é: “Se você experimentar algo — grave. Se gravar algo — faça upload. Se fizer upload de algo — compartilhe.”” (HARARI, 2016, p. 388-389).

nos artigos científicos, nos padrões de busca do *Google*, nas bases de dados das instituições (Banco Central, Banco Mundial, Serasa, IBGE, ONU) podem ser facilmente cruzados gerando graves riscos de violação aos direitos fundamentais.[74] Com a acessibilidade da tecnologias da informação, abre-se mão facilmente de dados e da privacidade para os aplicativos de relacionamento, de compras, de busca de dados, entre outros.

Tal agilidade na manipulação das informações pode dar origem a diversas ocorrências, desde a utilização de cadastros para apurar consumidores inadimplentes, assim como pela administração pública para aprimorar o planejamento e implementação das políticas públicas, servindo até mesmo ao Estado para, no desempenho de seu poder de polícia, por meio de um serviço de inteligência, dispor de informações sobre indivíduos que tenham atentado contra a ordem pública.

O grau de ascensão das novas tecnologias avança a passos largos a ponto de termos conhecimento biológico e capacidade de computação para criar algoritmos capazes de entender os humanos melhor que eles podem entender a si próprios. Com base no DNA, na pressão arterial, na função cerebral, o algoritmo é capaz de entender os sentimentos e escolhas melhor que a própria pessoa, podendo dizer: 'você quer isso e eu posso dizer por quê', como aponta Harari (2016).

A título exemplificativo, Harari (2016, p. 346) menciona que os "dispositivos como o Kindle, da Amazon, são capazes de coletar dados de seus usuários enquanto eles estão lendo o livro." Antes, quando alguém queria escolher um livro, dirigia-se à livraria. Ninguém sabia quem você era nem lhe recomendava nada. Agora, a *Amazon* faz isso por você. E, se o leitor conectar um *Kindle* a um *software* de reconhecimento facial ou a sensores biométricos no seu corpo, a *Amazon* estará perto de saber o impacto emocional exato de cada sentença que é lida. Com esse conhecimento, será capaz de dizer não apenas o que fazer na vida, mas também pressionar botões emocionais e manipulá-lo numa extensão muito maior que qualquer ditador com que

---

[74] Nesse sentido, "[...] o desenvolvimento tecnológico proporciona o aparecimento de novos instrumentos de violação de direitos fundamentais capazes de atuar em duas frentes: por um lado, por meio da identificação, rastreamento, monitoramento e análise de informações relativas aos detalhes da vida íntima e da identidade das pessoas; por outro, em razão das práticas de coleta, armazenamento, processamento, individualização e classificação das pessoas em determinados grupos. Como resultado, tais práticas modificam as relações de visibilidade/opacidade, que não devem ser compreendidas apenas como um atributo físico do sentido humano – o olhar –, mas, de maneira mais abrangente, como a ampla disponibilidade de informações personalizadas e compiláveis sobre indivíduos e grupos." (BOLZAN DE MORAIS; JACOB NETO, 2018, p. 94).

pudéssemos sonhar, afirma Harari em entrevista concedida à Folha de São Paulo. (LEITE, 2016).

No campo das relações laborais, a situação não é diferente. O surgimento das NTIC, principalmente a *internet*, vem se consolidando e alterando a própria forma de comunicação, tornando-se mais instantânea e plural, ensejando novos desafios, especialmente porque o trabalhador passa a ser instrumentalizado, considerado uma verdadeira fonte de informação pessoal. Segundo Rodotà (2008, p. 07),

> [...] nas sociedades de informação, como são as sociedades em que vivemos, pode-se dizer que 'nós somos as nossas informações', pois que elas nos definem, nos classificam, nos etiquetam.[75]

Contudo, embora se viva na chamada sociedade da informação, não se pode ignorar o fato de que as inovações tecnológicas estão assumindo características de controle praticamente ilimitadas[76], podendo originar discriminações e conduzir rapidamente para uma condição bem mais preocupante, a chamada sociedade da vigilância[77], como alerta Stefano Rodotà, em sua obra 'A vida na sociedade da vigilância: a privacidade hoje'.

---

[75] Dessa forma, "a sistemática coleta e processamento dos fluxos de informação possibilita a classificação pouco – ou nada – democrática das pessoas em categorias sociais de seu interesse. Com base na análise das informações de uma troca de *e-mails*, por exemplo, é possível – sem sequer ter acesso ao conteúdo da mensagem – classificar indivíduos em grupos específicos, classificações estas que possuem consequências significativas para suas vidas. A categorização dos seres humanos tem como finalidade a sua inclusão ou exclusão em determinados grupos. [...]" (BOLZAN DE MORAIS; JACOB NETO, 2018, p. 87).

[76] "[...] na atualidade a internet é uma zona livre e sem lei que desgasta a soberania do Estado, ignora fronteiras, elimina a privacidade e representa o mais formidável risco à segurança global. Não obstante, uma década atrás isso quase não fosse captado nos radares, no presente já se ouvem previsões histéricas de um iminente Onze de Setembro cibernético. Em consequência, governos e ONGs estão promovendo intensos debates sobre a reestruturação da *internet*, mas é muito mais difícil mudar um sistema existente do que intervir enquanto está sendo concebido. Além disso, enquanto a desajeitada burocracia governamental fica matutando a respeito de uma regulação cibernética, a internet se metamorfoseou dez vezes. A tartaruga governamental não é capaz de se emparelhar com a lebre tecnológica. Ela é soterrada pelos dados." (HARARI, 2016, p. 377).

[77] Na visão de Bolzan de Morais e Jacob Neto (2018), a ideia de vigilância continua existindo, porém, dado o complexo fenômeno que estamos vivendo, marcado por um mundo globalizado e interconectado, com novas tecnologias e formas de organização social, especialmente a fluidez e a descentralização, entra em cena uma nova categoria, a *surveillance*, a qual não pode ser traduzida como "vigilância", pois embora a tradução literal – vigilância – seja linguisticamente adequada, a palavra em língua inglesa – bem como na francesa – possui uma polissemia que não é alcançada pelo termo em português. O "novo conceito de *surveillance* pode ser caracterizado, especialmente, pelo uso de "sentidos estendidos", ou seja, pela utilização de meios técnicos capazes de extrair ou criar informações pessoais. Tais informações não são apenas "sobre indivíduos", dado que também consideram o contexto da sua coleta, o que permite afirmar que boa parte da *surveillance* está ligada ao reconhecimento de padrões relacionais do indivíduo com outros e com o espaço. [...] Assim, um dos processos-chave para caracterizar a *surveillance* é o atual uso de bancos de dados indexáveis no processamento de informações para diversas finalidades. Entende-se, portanto, que as novas

Para o mercado, inegável que as novas tecnologias produzem facilidades, ganhos de produtividade, melhores condições de convívio social e laboral, aumento da criatividade, otimização do tempo, espírito colaborativo e engajamento. Por outro lado, estas mesmas tecnologias, sobretudo a *internet*, podem ensejar inúmeras desvantagens, nomeadamente:

> por filtrar informações a terceiros relativas a segredo empresarial ou informações sobre clientes da empresa, facultar o assédio a um companheiro de trabalho e realizar acções que podem comprometer a imagem, a credibilidade e a própria subsistência da empresa. Pode ainda falar-se, nomeadamente, de problemas de segurança, atendendo a que os sistemas de informação, actualmente, são vitais para as empresas. (MOREIRA, 2012, p. 23).

Em uma sociedade cada vez mais competitiva e global, a preocupação em torno das NTIC faz sentido, pois estão modificando substancialmente não só a sua estrutura das empresas, mas também processos de reestruturação, provocando uma mudança significativa no comportamento quotidiano dos trabalhadores no próprio local de trabalho. (MOREIRA, 2012). A fim de subsistir, as empresas precisam sempre atualizar sua tecnologia e aumentar o conhecimento, inclusive o trabalhador precisa estar atualizado quanto às novidades, "para não ser excluído, tem de ter obrigatoriamente um *QI* numérico mínimo que lhe permita conhecer, sobreviver e conseguir trabalhar com estas NTIC." (MOREIRA, 2012, p. 25).

Para os trabalhadores (que também são usuários da *internet*), embora as NTIC tragam vantagens para o desempenho das atividades laborais, a facilidade de navegação na rede mundial de computadores, com inúmeras trocas de informações, concedeu um enorme número de informações de caráter pessoal, permitindo ao empresário o conhecimento completo do seu perfil,[78] que vai desde aspectos

---

infraestruturas da tecnologia da informação, ao permitirem o processamento em tempo real e o armazenamento ilimitado de dados, não apenas "qualificam" a vigilância, mas introduzem mudanças qualitativas que permitem um "salto" em direção ao conceito de *surveillance.* [...] A *surveillance*, muito além de uma vigilância, é uma das grandes marcas das sociedades contemporâneas e depende intrinsicamente do uso dos bancos de dados pessoais. Dependemos dela para nos mover pelo mundo cotidiano. (BOLZAN DE MORAIS; JACOB NETO, 2018, p. 90-91).

[78] Bolzan de Morais e Jacob Neto (2018, p. 94) referem que "a coleta, o armazenamento e o processamento automatizado de diversas informações sobre os indivíduos e grupos – transações financeiras, ligações telefônicas, preferências de consumo, hábitos de uso da *internet*, etc. – permite, além da territorialidade, transcender também a temporalidade, uma vez que, embora estejam relacionadas ao presente, as novas técnicas de *surveillance* empregam o armazenamento quase ilimitado de informações – passado – e o seu uso por ferramentas de análise estatística e de predições de risco – futuro." No caso, os autores se referem à previsão de comportamentos, a qual pode ser adotada pelo poder público, para prever atitudes terroristas, por exemplo, ou pela iniciativa privada,

estritamente profissionais a características individuais pertencentes ao âmbito da sua privacidade. Em consequência, a barreira que havia entre vida privada e vida profissional deixa de existir, dando origem a problemas de conciliação entre os direitos à privacidade e à liberdade de expressão dos trabalhadores e os direitos do empregador.

> A utilização de dados pessoais, em especial dos chamados dados "sensíveis" – histórico clínico, orientação religiosa, política e sexual, histórico trabalhista e outros – em bancos de dados informatizados tornou possível a descoberta de aspectos relevantíssimos da intimidade dos cidadãos. Esta possibilidade cresce muito mais quando são utilizados os banco de dados cruzados, ou seja, ao serem relacionadas informações de diversos bancos de dados. Tal uso pode ter como objetivo o controle social operado por um Estado ou organizações totalitárias, ou mesmo fornecer indicativos de um futuro comportamento para um comerciante ou para um provável empregador. É evidente que isto implica em um atentado frontal à privacidade individual, possível sem que se usem microfones nem câmaras, apenas recolhendo as informações que todo cidadão costuma revelar nas mais diversas ocasiões, como o cadastro que faz em uma locadora de vídeos ou sua ficha em uma clínica médica. (DONEDA, 2000, p. 06).

Assim, muitos são os perigos, reais e potenciais, que as NTIC oferecem aos direitos fundamentais do trabalhador. As situações envolvendo decisões exclusivamente automatizadas[79], o tratamento de dados pessoais e sensíveis na seleção, no curso e no término da relação laboral, a violação à privacidade e à intimidade, a utilização de banco de dados como mecanismo para implementar o controle dos trabalhadores, a criação de perfis, todas essas são apenas algumas das inúmeras hipóteses que podem ensejar discriminação, exclusão e perseguição aos trabalhadores.

---

para melhor conhecer os consumidores. Tal prática, contudo, tem atraído a atenção das empresas, especialmente ao promoverem a contratação de trabalhadores, pois, como aduzem os autores, o homem sendo "um animal de hábitos, de maneira que, com a coleta de informações diversas durante período de tempo suficiente, é possível prever padrões de comportamento, deslocamento, preferências e interação social." (BOLZAN DE MORAIS; JACOB NETO, 2018, p. 95).

[79] As decisões exclusivamente automatizadas correspondem à capacidade de tomar decisões através de meios tecnológicos e sem intervenção humana, podendo basear-se em qualquer tipo de dados, como, por exemplo, dados fornecidos diretamente pelas pessoas em causa (tais como respostas a um questionário), dados observados acerca das pessoas (tais como dados de localização recolhidos por meio de uma aplicação) ou dados obtidos ou inferidos, tais como um perfil da pessoa que já tenha sido criado (ex: uma pontuação de crédito). (COMISSÃO EUROPEIA, 2017). Com relação ao tema, o Repertório de Recomendações Práticas da OIT sobre a proteção de dados pessoais dos trabalhadores informa que não rejeita o uso de procedimentos automatizados, podendo os empregadores utilizá-los para preparar suas discussões, desde que como meio auxiliar. Porém, posiciona-se contrário a que as decisões sejam tomadas unicamente com base no tratamento automatizado de dados pessoais, pois admitir isso seria reconhecer que os trabalhadores não têm direito a um tratamento justo. (OIT, 1997).

Estima-se que 4,1 bilhões de pessoas tenham acesso à *internet* no mundo e que 3,4 bilhões mantenham uma rede social (CIRIACO, 2018). Logo, grande parte da população tem suas informações na rede mundial. E todo esse banco de dados disponível na rede é utilizado pelas empresas (dada a facilidade de acesso), especialmente na fase de admissão, quando alguém se candidata a uma vaga, sendo checadas as redes sociais para a análise dos currículos e obtenção de maiores informações pessoais e profissionais dos candidatos.[80]

> Desde logo, na fase de acesso e formação do contrato de trabalho, são os próprios candidatos a fornecerem, ainda que involuntariamente, muitas das informações profissionais assim como outras extremamente privadas, em redes sociais, como o *Facebook*, *Orkut*, *Twitter*, *Linkedin* ou o *Myspace*.
> Neste *Mundo Novo do Trabalho*, que de admirável, por vezes, parece ter muito pouco, é frequente a *googalização* de todos, na medida em que auxilia quem faz o processo de selecção. Através de uma pesquisa à distância, extremamente rápida, de forma gratuita, e sobretudo discreta, é possível conhecer a intimidade de terceiros pois frequentemente estes dados, por vezes extremamente privados, encontram-se em acesso livre.
> Actualmente muitas empresas recorrem a estas redes como um *complemento* na avaliação dos candidatos de forma a tentar identificar quem tem o *melhor perfil*.
> Tratam-se das novas "impressões digitais", relacionadas com os mais diversos sectores: pessoal, profissional, político, social, que vão deixando vestígios em vários locais e que através de uma pesquisa em motores específicos permitem construir perfis dos trabalhadores. O fantasma do *Big Brother*, que todos poderíamos identificar e que controlava tudo, parece *artesanal*, quando comparado com estes inúmeros "Little Brothers", que conseguem seguir as pessoas e conhecê-las ao mais ínfimo detalhe. Defende-se, desta forma, que perante este *Admirável Mundo Novo do Trabalho*, é necessário reflectir sobre a eventual necessidade de um "*habeas corpus* numérico", que permita um controlo real e efectivo sobre os dados pessoais, assim como a possibilidade real da sua eliminação. (MOREIRA, 2012, p. 26).

A título ilustrativo, Schreiber (2013) refere em sua obra 'Direitos da personalidade', o caso de uma companhia que coleta em redes sociais dados sobre os candidatos selecionados para uma entrevista de emprego. Pode a companhia se valer desses dados para eliminar certo candidato que se declara integrante de um movimento sindical ou membro fanático de uma torcida organizada, ou por publicar

---

[80] Antes mesmo do surgimento dos computadores, a prática do tratamento de dados para fins de seleção de profissionais já ocorria. Nesse sentido, Danilo (2000) menciona o exemplo trazido pelo professor italiano Alessandro Bellavista, o qual destaca o caso do fabricante de automóveis FIAT que, entre 1948 e 1971, selecionou 350.000 dos seus empregados com base em dados sigilosos do SIFAR (antigo serviço secreto militar italiano), evitando a contratação de pessoas com tendências políticas de esquerda, uma vez que a Itália, em 1954, por meio do seu Conselho Ministerial decidiu iniciar uma política de discriminação contra os comunistas e seus aliados, com base em informações colhidas sobre a fé política dos italianos.

uma frase infeliz na *internet* ou postar uma foto mais ousada que possa sugerir “comportamento incompatível com o perfil da empresa”. O destino do candidato “acaba decidido não com base na sua real personalidade, mas com base na representação virtual que é construída a partir de dados pessoais coletados de modo mais ou menos aleatório.” (SCHREIBER, 2013, p. 138).

A incorporação das NTIC para reunir informações sobre trabalhadores e promover uma seleção baseada em dados é uma realidade presente, sobretudo nas grandes empresas, sendo o caso mais emblemático o da empresa *Amazon.com*, a qual utilizou a automação de dados para recrutar candidatos. O caso ganhou repercussão internacional depois que a companhia reconheceu que o sistema promovia discriminação de gênero contra mulheres candidatas para o desempenho das funções de desenvolvedor de *software* e outros cargos técnicos na empresa. (RUBIO, 2018).

Assim, na sociedade da informação, as empresas utilizam-se das novas ferramentas para atender seu interesse empresarial de aprimorar a produção e a tomada de decisões quanto à contratação, promoção e dispensa de trabalhadores. Tais interesses sempre existiram e são legítimos (desde que exercidos em conformidade com o direito), estando amparados nas faculdades organizativas empresariais.

O grande problema é que todos os inúmeros dados aparentemente sem importância e exclusivamente pertencentes ao seu proprietário são deixados na rede, podendo ser agregados, permitindo a construção de perfis. E, em relação aos trabalhadores, “torna-se muito fácil reconstruir praticamente tudo, nomeadamente através da recolha de textos, vídeos e fotografias que vão deixando na *Web*.” (MOREIRA, 2012, p. 27).

Ainda quanto aos riscos no âmbito das relações laborais, não se pode esquecer que a informação “mesmo a mais pessoal, circula de forma muito rápida, em muito maior quantidade e através de muitos mais sujeitos do que em qualquer outra época, aumentando o perigo da sua descontextualização.” (MOREIRA, 2012, p. 17). Assim, é comum durante a vigência do contrato, as empresas acumularem um grande número de informações sobre a vida de cada trabalhador. Porém, não raramente, acontecem vazamentos e compartilhamentos destas informações entre as próprias

empresas ou até mesmo para fora, com graves consequências para o trabalhador, como a divulgação das chamadas ‘listas negras’ ou ‘listas discriminatórias’.[81]

Além disso, com a tecnologia existente e a difusão de informações, é possível acessar dados pessoais e sensíveis dos trabalhadores (como opiniões políticas, filiação a sindicato, orientação sexual ou religiosa, origem racial ou étnica), com fundamento em estatísticas baseadas no local de residência, no consumo de informações e na reputação *online*, que vão muito além do necessário para apurar uma mera aptidão profissional, mas que podem contribuir para motivar desigualdades e discriminações no mundo do trabalho. Como alude Doneda (2000, p. 06):

> A facilidade com que podem e cada vez mais poderão ser obtidas informações pessoais lança, porém, uma sombra sobre a privacidade, capaz de gerar, como potencial conseqüência, a diminuição da esfera de liberdade do ser humano. Numerosos outros fatores se agregam, o que pode ser exemplificado pelos efeitos da pesquisa atualmente realizada pelo Projeto Genoma, destinado a mapear o código genético humano e, assim, proporcionar um tratamento que de outra forma seria impossível para diversas patologias. O uso indiscriminado de informações genéticas pessoais, obtidas graças à técnica desenvolvida pelo projeto, por potenciais empregadores, em um único exemplo, pode determinar a exclusão incontinenti desta pessoa do mercado de trabalho e mesmo privá-la de uma vida digna se por acaso possuir predisposição genética para determinada doença.

Dessa forma, as informações obtidas a respeito dos trabalhadores, se de um lado servem para facilitar a gestão cotidiana do contrato de trabalho, de outro, também servem para traçar o perfil profissional do empregado[82] e apoiar a tomada de decisões das empresas. A disponibilidade generalizada de dados pessoais na *internet*, somada à capacidade para encontrar correlações e criar ligações,

---

[81] Trata-se de uma “prática crescente no mercado de trabalho, posto que facilitada pelo advento das novas tecnologias, consistente na associação do nome de candidato a emprego, ou empregado, a determinadas características pessoais capazes de representar óbice ao acesso ao trabalho ou manutenção do direito ao trabalho. Isso porque, através dessa listagem, que normalmente circula entre empregadores, ou então através das agências de colocação, armazenam-se e circulam-se informações relativas àqueles empregados que tenham promovido reclamação trabalhista perante seus ex-empregadores, ou ainda fazendo-se constar outras informações diversas como significativa atividade sindical, dentre outras.” (WEINSCHENKER, 2013, p. 59).

[82] “Em termos genéricos, a definição de perfis significa a recolha de informações sobre uma pessoa (ou um grupo de pessoas) e a avaliação das suas características ou dos seus padrões de comportamento, a fim de a inserir em determinada categoria ou grupo, nomeadamente para fins de análise e/ou previsão, por exemplo, da sua capacidade para executar uma tarefa, dos seus interesses ou do seu comportamento presumível. [...] A definição de perfis corre o risco de ser abusiva e gerar discriminação, por exemplo, ao impedir o acesso de pessoas a oportunidades de emprego, crédito ou seguros, ou ao serem-lhes dirigidas ofertas de produtos financeiros com riscos ou custos excessivos.” (COMISSÃO EUROPEIA, 2017, p. 08 e 11).

possibilitam determinar, analisar e prever aspectos que digam respeito à personalidade ou ao comportamento, aos interesses e aos hábitos de uma pessoa. Tal método tem diversas aplicações, inclusive para fins de seleção de trabalhadores. Contudo, a definição de perfis, como visto, pode gerar riscos significativos para os direitos e as liberdades fundamentais das pessoas, que exigem garantias adequadas:

> A definição de perfis é suscetível de perpetuar os estereótipos existentes e a segregação social. Pode igualmente amarrar as pessoas a uma categoria específica e limitá-las às respetivas preferências sugeridas, pondo assim em causa a sua liberdade para escolher, por exemplo, determinados produtos ou serviços, tais como livros, música ou fluxos de notícias. Em certos casos, a definição de perfis é suscetível de resultar em previsões imprecisas. Noutros casos, poderá dar origem a uma negação de serviços e bens e a uma discriminação injustificada. (COMISSÃO EUROPEIA, 2017, p. 06).

Como mencionado, com as potencialidades da análise de megadados, da inteligência artificial e da aprendizagem automática cada vez mais desenvolvidas, tornou-se possível monitorar, registrar e cruzar dados e informações à distância, de forma sistemática, capaz de traçar perfis profissionais e pessoais de qualquer trabalhador. Ocorre que o poder conferido ao empregador pelos meios informatizados, quando usados como instrumento de limitação, supressão ou até mesmo de eliminação de certas garantias individuais, coloca em risco direitos e garantias fundamentais.

O empregador não pode controlar tudo a todo o tempo. A subordinação jurídica no âmbito das relações laborais, quando confrontada com a utilização das tecnologias e com o tratamento de dados do trabalhador, deve se adequar às exigências legais atinentes ao regime de proteção de dados, associada aos princípios da finalidade, da adequação, da necessidade, da transparência, da segurança, da proporcionalidade e da boa-fé, assim como com os direitos de informação, de acesso e de oposição.[83]

Disso decorre a importância do estudo da proteção aos dados pessoais e sensíveis, tanto em âmbito internacional, como no ordenamento jurídico brasileiro, passando pela fixação dos princípios como um norte a guiar o reestabelecimento do equilíbrio entre os poderes do empregador e os direitos e liberdades do trabalhador,

---

[83] Quanto às mencionadas categorias jurídicas, remete-se o leitor aos itens 3.2 e 3.3 para maior aprofundamento.

culminando na consolidação da proteção aos dados como um direito fundamental, temas estes que serão objeto do próximo capítulo.

3 A PROTEÇÃO AOS DADOS PESSOAIS E SENSÍVEIS DO TRABALHADOR COMO DIREITO FUNDAMENTAL

A concepção da proteção dos dados pessoais e sensíveis como um direito humano fundamental vem ganhando projeção no cenário jurídico. A preocupação em torno dos dados[84] tem aumentado consideravelmente em decorrência do avanço tecnológico observado nas últimas décadas. A disponibilização, o tratamento e a combinação de informações tornam-se cada vez mais intensos, a ponto de resultar em uma sociedade gradativamente orientada por dados.

Na atualidade, as questões envolvendo violação da privacidade, da intimidade e dos dados são progressivamente presentes. Paralelo a isso, no âmbito das relações laborais, esfera de interesse da presente pesquisa, os riscos aos direitos e liberdades fundamentais dos trabalhadores são crescentes.

Nesse contexto, ganha relevo o tema da proteção aos dados pessoais e sensíveis, essencial para a proteção humana da pessoa-trabalhadora, como um novo direito fundamental que garante aos seus titulares a capacidade de dispor de seus dados e controlar o uso que deles é feito.

Diante disso, neste capítulo será abordada a tutela aos dados pessoais e sensíveis no sistema normativo europeu e no ordenamento jurídico brasileiro, dada a influência do Regulamento Geral de Proteção de Dados da União Europeia na aprovação da Lei nº 13.709/2018, conhecida como a Lei Geral de Proteção de Dados Pessoais (LGPD).

Na sequência, serão abordados os principais princípios que norteiam o tratamento dos dados e de que forma eles podem ser aplicados nas relações laborais a fim de assegurar aos trabalhadores uma proteção adequada e, por fim, será desenvolvido o tema da proteção aos dados como um direito fundamental da pessoa-trabalhadora, na medida em que seus dados configuram expressão direta da própria personalidade.

---

[84] Tal preocupação se deve pelo fato de os dados pessoais serem "*fuente de riesgos para las personas, no sólo por lo que revela acerca de su identidad y de sus rasgos característicos sino también por las ocasiones que brinda de afectación a su intimidad o su vida privada*." (MURCIA; CARDO, 2019, p. 01). [...] fonte de riscos para as pessoas, não somente pelo que revela sobre sua identidade e suas características, mas também pelas ocasiões em que isso afeta sua a privacidade ou sua vida privada. (tradução nossa).

3.1 A TUTELA DOS DADOS PESSOAIS E SENSÍVEIS NO SISTEMA EUROPEU

O avanço das tecnologias de informação com maior vigor na Europa e na América do Norte fez com que a comunidade jurídica destes territórios se ocupassem do tema da proteção dos dados antes dos chamados países em desenvolvimento. Daí por que a relevância de estudar a experiência estrangeira, particularmente a do sistema europeu[85], antes de adentrar no contexto brasileiro.

Sobre a evolução tecnológica na área da informação:

> 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[86] 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"[87] sobre o tratamento automático de informação. (DONEDA, 2000, p. 15).

Contudo, frente à multiplicação dos centros de processamento e o baixo custo dos computadores, as leis de primeira geração tornaram-se inoperantes. Ao lado destas disposições legais surgiram outras iniciativas, como a da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) em 1980 e do Conselho da Europa em 1981 que adotaram dois instrumentos na área, respectivamente, as

---

[85] A escolha pelo sistema europeu deve-se ao fato deste ter servido de modelo para o sistema brasileiro de proteção de dados, o que será aprofundado no item 3.2.

[86] Sobre o direito à proteção de dados pessoais, Ruaro e Rodriguez (2010, p. 167) apontam que “podem ser descritos como seus antecedentes históricos tanto o artigo 12 da Declaração Universal dos Direitos do Homem, como o artigo 8º do Convênio para Proteção de Direitos Humanos e Liberdades Fundamentais, pactuado em Roma, no ano de 1950. Figuram também nesta lista de influências os artigos 17 e 18 do Pacto de Direitos Civis e Políticos, firmado em Nova Iorque no ano de 1966.” Para maior aprofundamento, a Declaração Universal dos Direitos do Homem está disponível em: https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf; a Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais está disponível em: https://www.echr.coe.int/Documents/Convention_POR.pdf, e o Pacto Internacional sobre os Direitos Civis e Políticos está disponível em: http://www.cne.pt/sites/default/files/dl/2_pacto_direitos_civis_politicos.pdf.

[87] As leis de primeira geração “tinham como característica o fato de basearem a tutela da privacidade dos bancos de dados no controle da autorização dada ao seu funcionamento.” (DONEDA, 2000, p. 15).

Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais[88] e a Convenção nº 108/1981[89] (RODOTÀ, 2008).

Como explica Doneda (2000), com o surgimento dos microcomputadores, da *internet* e da difusão dos bancos de dados informatizados, uma segunda geração de leis teve início na segunda metade da década de 70, cujo mecanismo de autorização para funcionamento se apresentava diluído e substituído, em muitos casos, por uma mera notificação de sua criação.

Posteriormente, a terceira geração de leis surgiu a partir da década de 80 e refletia a proliferação dos bancos de dados e a necessidade de uma tutela flexível, impossível de ser estabelecida por leis que se pretendiam definitivas, dada a dinâmica do avanço tecnológico. Apesar disso, nelas é possível identificar alguns princípios comuns (princípio da publicidade ou da transparência, princípio da boa-fé ou da finalidade, princípio do livre acesso e princípio da segurança física e lógica), presentes em diversos graus.

Ocorre que o vertiginoso desenvolvimento das ferramentas tecnológicas e a criação de *softwares* específicos de gestão de dados passaram a permitir o armazenamento e tratamento instantâneo de milhares de dados, ensejando a necessidade da criação de mecanismos normativos de proteção dos dados.

Frente a este cenário, a Comunidade Europeia criou a Diretiva nº 95/46/CE[90], de 23 de novembro de 1995, que constitui o texto de referência em

---

[88] Trata-se do documento que estabeleceu diretrizes para proteção e coleta de dados, de maneira não impositiva, aos países-membros da OCDE, ou seja, corresponde ao "primeiro instrumento relativo à proteção de dados classificado como *soft law* no campo do direito internacional. O referido documento, apesar de não vinculativo, influenciou de maneira determinante os Estados-Membros da OCDE a incluírem em seus ordenamentos jurídicos regras gerais de proteção de dados." (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.

[89] Dispõe sobre a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal. Trata-se do "primeiro texto jurídico unificado sobre a matéria, que se propôs a garantir no território de cada país-membro, o respeito aos diretos e liberdades fundamentais de todas as pessoas, independentemente de suas nacionalidades ou residências." (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.

[90] Regulamentou o tratamento de dados pessoais e a livre circulação destes no âmbito da comunidade europeia, com enfoque nos direitos fundamentais. Trata-se de uma Diretriz que 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. Além disso, 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. Apesar de não apontar direitos atinentes à proteção de dados pessoais e quais seriam seus limites, a norma apresentou princípios que deveriam ser observados nas legislações internas para possibilitar a defesa dos interesses protegidos. (DONEDA,

matéria de proteção de dados pessoais em âmbito europeu[91]. A partir de então, os países integrantes da Comunidade Europeia criaram suas leis internas de proteção de dados.[92] Em 1997, surgiu a Diretiva nº 97/66/CE, relativa ao tratamento de dados de caráter pessoal e da proteção à intimidade no setor das telecomunicações.[93] Em 2002 foi elaborada a Diretiva nº 2002/58/CE dedicada ao tratamento de dados pessoais e à proteção à intimidade no setor de comunicações eletrônicas.[94] E, por último, em 2006, sobreveio a Diretiva 2006/24/CE, que dispõe sobre a conservação

---

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.

[91] Antes mesmo da criação da Diretiva nº 95/46 e do Convênio nº 108/1981, muitos países europeus já haviam editado leis regulamentando a proteção de dados. Na Europa Ocidental, a Suécia foi o primeiro país a criar uma lei modelo para a proteção das liberdades frente à informática, a chamada *Datalag* ou lei sobre dados, de 11 de maio de 1973, dando origem ao organismo supervisor *Data Inspektion Board* (DIB). Trata-se da primeira lei no mundo promulgada exclusivamente contra os perigos políticos da informatização. A França, por sua vez, em 1974, criou a 'Comissão de Informação e Liberdades', a qual produziu um relatório sobre a informatização da sociedade (Relatório Tricot), que inspirou a edição da Lei sobre Informática, Arquivos e Liberdades de 1978, que também formou a Comissão Nacional de Informática e Liberdades, responsável pelo cumprimento da lei. Após, a Alemanha Federal instituiu em 1976 um comissário federal de dados responsável por velar pelo cumprimento dos direitos a eles relativos. (CANO, 1994). Na sequência, a Espanha, em 1992, editou a Lei Orgânica de Regulação do Tratamento Automatizado dos Dados de Caráter Pessoal (Lortad), que, assim como as outras leis, trouxe definições, princípios e direitos sobre o uso e tratamento de dados pessoais e sensíveis, além de criar uma agência pública para, administrativamente, resolver questões referentes ao uso desses dados. Na mesma linha, em 1988, o Reino Unido editou o *Data Protection Act* (DPA) e criou o *Information Commissioner's Office* (ICO), órgão responsável por proteger a informação pessoal. Além desses, Suíça (1992), Itália (1997), Áustria, Dinamarca, Holanda, Noruega (2000) e Bulgária (2001), também adotaram regulamentações sobre o uso de dados pessoais. (CHEHAB, 2012).

[92] Doneda (2000) refere que mesmo países excluídos do bloco de vanguarda tecnológica e da liderança da produção das tecnologias de informação, como o caso de Portugal, previa em sua Constituição da República, de modo expresso, meios jurídicos de proteção dos dados pessoais de seus cidadãos, como se observa no artigo 35, que trata da utilização da informática: "1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei. 2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente. 3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis. 4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei. 5. É proibida a atribuição de um número nacional único aos cidadãos. 6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional. 7. Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei." (PORTUGAL, Constituição da República Portuguesa de 1976).

[93] Esta Diretiva foi revogada e substituída pela Diretiva 2002/58/CE. A Diretiva nº 97/66/CE está disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31997L0066&from=PT.

[94] Em que pese não tenha inovado o ordenamento da comunidade europeia, tal normativa permitiu a adequação das finalidades presentes na Diretiva 95/46/CE à realidade tecnológica não presente à época de sua promulgação. (DONEDA, 2006). A Diretiva nº 2002/58/CE está disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32002L0058&from=PT.

de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrônicas publicamente disponíveis ou de redes públicas de comunicações, a qual salienta a necessidade da tutela do direito à privacidade e intimidade por parte dos Estados-membros.

De acordo com Doneda (2006, p. 227), tais Diretivas representaram "um padrão mínimo de proteção em toda a área da União Europeia", desenvolvidas a partir da experiência de alguns países europeus que já haviam legislado sobre a matéria.

Ainda em território europeu, menciona-se a Carta dos Direitos Fundamentais da União Europeia, de 7 de dezembro de 2000, a qual reconheceu a proteção de dados como um direito autônomo[95], podendo este ser considerado o último ponto de uma longa evolução, separando a privacidade da proteção de dados.[96] (RODOTÀ, 2008). Nessa perspectiva, o direito à proteção de dados pode ser entendido como:

> O poder que a pessoa tem de dispor dos dados e controlá-los, decidindo quais deles fornecerá a um terceiro, seja um particular ou o Estado, a fim de saber quem os possui, contando a todo o momento com a faculdade de acessá-los, retificá-los, cancelá-los ou opor-se a sua posse ou uso.[97] (GONZÁLEZ; GAMBOA, 2018, p. 223, tradução nossa).

Mais recentemente, em 2016, o Parlamento Europeu aprovou o Regulamento Geral de Proteção de Dados da União Europeia (RGPD) ou *General Data Protection Regulation* (GDPR), o qual entrou em vigor em 25 de maio de 2018.

---

[95] Nesse sentido, a Carta dos Direitos Fundamentais da União Europeia reconheceu em seu artigo 8 que "Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito." (UNIÃO EUROPEIA, 2000). Acerca do artigo 8, Rodotà (2008, p. 17) pondera que este "deve ser colocado num contexto mais amplo da Carta, que se refere aos novos direitos surgidos das inovações científicas e tecnológicas. O artigo 3 lida com o "direito à integridade da pessoa", *i.e*., a proteção do corpo *físico*; o artigo 8 lida com a proteção de dados, *i.e*., o corpo *eletrônico*. Estas provisões são diretamente relacionadas à dignidade da pessoa humana – que o artigo 1º da Carta declara ser inviolável – assim como à declaração feita no preâmbulo da Carta, por meio da qual a comunidade "coloca a pessoa no coração de suas atividades". Daí que a proteção de dados contribuiu para a "constitucionalização da pessoa" – o que pode ser considerado como uma das mais significativas conquistas, e não apenas da Carta. Estamos diante da verdadeira reinvenção da proteção de dados – não somente porque ela é expressamente considerada como um direito fundamental autônomo, mas também porque se tornou uma ferramenta essencial para o livre desenvolvimento da personalidade. A proteção de dados pode ser vista como a soma de um conjunto de direitos que configuram a cidadania do novo milênio."

[96] "Assim, no contexto da União Europeia, diversos países têm considerado a privacidade das informações pessoais como direito fundamental autônomo, por ser manifestação da própria personalidade." (WEINSCHENKER, 2013, p. 19).

[97] [...] *el poder que tiene la persona de disponer de ellos y controlarlos, decidiendo cuáles proporcionará a un tercero, ya sea un particular o el Estado, para así saber quién los posee, contando en todo momento con la facultad de acceder a ellos, rectificarlos, cancelarlos u oponerse a su posesión o uso.*

Trata-se da mais importante normativa sobre o tema da proteção de dados em âmbito mundial[98], instituída em substituição à Diretiva 95/46/CE, mas que se manteve "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." (SCHREIBER, 2018). O objetivo do RGPD foi "adequar a proteção já existente a um cenário com grandes agentes e um fluxo de dados sem precedentes." (BRITTO; RIBEIRO, 2018, p. 388).

Apresentada esta breve síntese sobre a evolução histórica da tutela dos dados pessoais no sistema europeu, encaminha-se à definição do que são exatamente dados pessoais e sensíveis à luz de algumas dessas normativas internacionais.

O Conselho da Europa, por meio da Convenção nº 108/1981, definiu que os dados de caráter pessoal significam "qualquer informação relativa a uma pessoa singular identificada ou susceptível de identificação."[99] Em igual sentido, o RGPD, em seu artigo 4, item 01, define dados pessoais como a:

> 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, económica, cultural ou social dessa pessoa singular;[100] (UNIÃO EUROPEIA, 2016).

Portanto, o que identifica uma informação[101] como pessoal é quando o objeto da informação é a própria pessoa, ou seja, a informação possui um vínculo

---

[98] Em panorama apresentado pela Organização das Nações Unidas (ONU), no que tange à adoção de legislação para garantir a proteção de dados e privacidade no mundo, a ONU observa que há uma crescente atenção das autoridades acerca do tema, ao revelar que atualmente 58% dos países contam com legislação específica de proteção de dados e 10% destes estão em fase de discussão de projetos. Dos 107 países com legislação vigente, 66 são economias em desenvolvimento, sendo que nessa área, a Ásia e a África mostram um nível de adoção semelhante, com menos de 40% dos países com uma lei em vigor. (ONU, 2019).

[99] Artigo 2º da Convenção nº 108/1981.

[100] Partindo da análise do artigo 4º do RGPD, Giménez (2019, p. 06) destaca como novidade a inclusão de novas formas de identificar uma pessoa devido a avanços tecnológicos e sua aplicação no ambiente empresarial. Dentro do local de trabalho, menciona como exemplos a impressão digital como mecanismo de controle do absenteísmo ou pontualidade dos trabalhadores e a possibilidade de conhecer a localização destes através de cartões magnéticos.

[101] Quanto à utilização dos termos "informação" e "dado", o conteúdo de ambos os vocábulos se sobrepõe em várias circunstâncias, sendo que a doutrina não raro trata estes dois termos indistintamente. Tanto a "informação" quanto o "dado" servem para representar um fato, um

objetivo com ela. Tal distinção é fundamental para afastar outras categorias de informações que, embora se relacionem com uma pessoa, não são propriamente informações pessoais. Como exemplo, Doneda (2006) menciona as opiniões alheias sobre alguém e a sua produção intelectual, a qual não é *per se* informação pessoal (embora o fato de sua autoria o seja).

Quanto aos dados sensíveis, a Convenção nº 108/1981 estabeleceu que são aqueles "que revelem a origem racial, as opiniões políticas, as convicções religiosas ou outras, bem como os dados de caráter pessoal relativos à saúde ou à vida sexual."[102] O RGPD, no artigo 9º, item 01, ao dispor sobre o tratamento de categorias especiais de dados pessoais, referiu que os dados sensíveis correspondem àqueles que:

> [...] revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.[103] (UNIÃO EUROPEIA, 2016).

A doutrina, ao se debruçar sobre o tema, aponta que os dados sensíveis portam informações que, caso fossem conhecidas ou processadas, apresentariam um elevado potencial lesivo aos seus titulares, e não raro para uma coletividade (DONEDA, 2006). "A categoria de dados sensíveis é fruto de uma observação pragmática da diferença que apresentam o efeito do tratamento destes dados em relação aos demais." (DONEDA, 2006, p. 161). Contudo:

> [...] mesmo dados não qualificados como sensíveis, quando submetidos a um determinado tratamento, podem revelar aspectos sobre a personalidade de alguém, podendo levar a práticas discriminatórias. Tal argumentação leva,

---

determinado aspecto de uma realidade, contudo cada um carrega um peso particular. O "dado" tem uma conotação mais primitiva e fragmentada, uma espécie de informação em estado potencial, antes de ser transmitida, ao passo que a "informação" refere-se a algo além da representação contida no dado, na qual já se pressupõe uma fase inicial de depuração de seu conteúdo, daí que a informação carrega em si também um sentido instrumental, no sentido de uma redução de um estado de incerteza. (DONEDA, 2006).

[102] Artigo 6º da Convenção nº 108/1981.

[103] Segundo Giménez (2019, p. 07), "*Este tipo de datos requieren un tratamiento más cuidadoso por su especial sensibilidad. Por este motivo en la relación laboral se debe justificar su tratamiento por parte del responsable."* Este tipo de dado requer um tratamento mais cuidadoso pela sua sensibilidade especial. Por esta razão na relação de trabalho deve-se justificar o seu tratamento pelo responsável. (tradução nossa).

> em síntese, a concluir que um dado, em si, não é perigoso ou discriminatório – mas o uso que dele se faz pode sê-lo.[104] (DONEDA, 2006, p. 162).

Em igual sentido, Simón (2000, p. 162) alerta que:

> [...] o cruzamento de notícias dá origem a nova forma de agressão às liberdades públicas pois o cidadão registrado em determinado banco de dados está constantemente vigiado, o que afeta, de forma direta, aspectos mais sensíveis da sua intimidade e vida privada.

Apesar disso, a mera proibição da coleta e tratamento de dados pessoais sensíveis demonstra-se inviável, pois muitas vezes o uso destes é legítimo e necessário[105], além do que a própria razão de ser de alguns organismos estaria comprometida, caso não pudessem acessar tais informações. (DONEDA, 2006).

No que tange à proteção específica dos dados pessoais e sensíveis dos trabalhadores, tema objeto da presente pesquisa, menciona-se em âmbito internacional a existência de duas importantes normativas: o Repertório de Recomendações Práticas da OIT sobre a Proteção de Dados Pessoais dos Trabalhadores, de 1997, e a Recomendação do Comitê de Ministros do Conselho de Europa – Recomendação CM/Rec (2015)5, as quais dispõem sobre o tratamento de dados pessoais no contexto laboral.

Ambas são normativas sem caráter obrigatório, que limitam-se a efetuar recomendações, sem ter a pretensão de substituir a legislação nacional, os regulamentos, as normas internacionais de trabalho ou outras normas aceitas.[106] Todavia, embora ausente o caráter vinculativo, tais recomendações trazem importantes orientações, além de apresentarem um conjunto de normas específicas, com ampla gama de definições, princípios e determinações para o setor empregatício em matéria de tratamento de dados pessoais.[107] No tocante:

---

[104] Assim, "Importante atentar que um dado *prima facie* não sensível pode o ser por revelar, indiretamente, aspectos relacionados à origem étnica (ex., com o sobrenome), à orientação sexual (ex., com o nome do companheiro), a convicções religiosas (ex., com os nomes atribuídos aos filhos). (FRAZÃO; OLIVA; ABILIO, 2019, p. 680-681).

[105] Doneda (2006) exemplifica o caso da "pesquisa de caráter científico ou mesmo a atividade médica, para as quais a importância de trabalhar com todos os dados possíveis, inclusive os sensíveis, é capital."

[106] É o que dispõe o item 02 do Repertório de Recomendações Práticas da OIT ao estabelecer a sua finalidade.

[107] O estudo da proteção de dados no âmbito laboral se justifica por ser esta uma das áreas mais propensas e expostas ao uso e circulação de informações, o que se verifica em suas diferentes fases: desde a preparação ou conclusão do contrato, passando pela fase de execução e, até mesmo a fase pós-contratual, na qual ainda pode haver compromissos ou obrigações pendentes de conformidade.

> A preocupação da OIT é pertinente, uma vez que, na relação laboral, que engloba as fases pré-contratual, contratual e pós-contratual, há o recolhimento de inúmeros dados pessoais dos trabalhadores, que, se já são vulneráveis em razão de sua condição de dirigido na relação de trabalho, mais fracos se tornam diante da possibilidade de armazenamento, tratamento e transmissão destes dados via informática.[108] (STIVAL, 2015. p. 131-132).

Com relação ao Repertório de Recomendações Práticas, além de trazer orientações para o tratamento dos dados pessoais do empregado, tanto no setor público quanto no privado, seja no processamento de dados manual ou no automático, ele também estabelece algumas definições, com destaque para a concepção de dado pessoal do trabalhador:

> Por 'dado pessoal' entende-se toda informação relacionada a um trabalhador identificado ou identificável. Um trabalhador é identificável se, mediante a reunião de diferentes dados contidos em um ou vários arquivos ou documentos, puder se determinar a identidade desse trabalhador. As disposições do repertório não são aplicáveis ao uso pelo empregador de dados referentes a trabalhadores que já não podem ser identificados ou que são anônimos. O termo 'identificável' deve ser interpretado como maneira razoável. Por exemplo, o repertório não se aplica aos casos em que se requeira muito tempo e esforço para identificar o trabalhador a partir dos dados utilizados.[109] (OIT, 1997, p. 11, tradução nossa).

E a própria abrangência da palavra trabalhador:

Além disso, a atividade profissional também pode provocar ou gerar outros usos de dados pessoais, tal como ocorre, por exemplo, em relação à organização de trabalhadores ou empregadores para fins de representação e defesa de seus interesses profissionais ou, em geral, por ocasião do exercício do que é conhecido como autonomia coletiva. (MURCIA; CARDO, 2019, p. 09).

[108] O preâmbulo do Repertório de Recomendações retrata tal preocupação, na medida em que "*La utilización de técnicas informáticas de recuperación de datos, los sistemas automatizados de información relativa al personal, la vigilancia electrónica y los exámenes genéticos y toxicológicos ponen de manifiesto la necesidad de elaborar disposiciones para proteger los datos que se refieran específicamente a la utilización de los datos personales de los trabajadores con el fin de salvaguardar la dignidad de éstos, proteger su vida privada y garantizarles el ejercicio de su derecho fundamental a decidir quiénes podrían utilizar determinados datos, con qué finalidad y en qué circunstancias."* (OIT, 1997, p. 01). A utilização das técnicas informáticas de recuperação de dados, dos sistemas automatizados de informação relativo à pessoa, da vigilância eletrônica e dos exames genéticos e toxicológicos, tudo isso requer a elaboração de disposições para proteger os dados que se refiram especificamente ao uso de dados pessoais dos trabalhadores, a fim de salvaguardar a dignidade destes, proteger sua vida privada e garantir o exercício de seu direito fundamental de decidir quem poderá usar determinados dados, com que finalidade e em que circunstâncias. (tradução nossa).

[109] *Por 'dato peronal' se entiende toda información relativa a un trabajador identificado o identificable. Un trabajador es identificable si, mediante la reunión de diferentes datos contenidos en uno o en varios ficheros o documentos, se puede determinar la identidad de ese trabajador. Las disposiciones del repertorio no son aplicables al uso por el empleador de datos referidos a trabajadores que ya no pueden ser identificados o que son anónimos. El término 'identificable' debe ser interpretado de forma razonable. Por ejemplo, el repertorio no se aplica a los casos en los que se requeriría una gran cantidad de tiempo y esfuerzo para identificar al trabajador a partir de los datos utilizados*.

> No repertório o termo abrange não apenas trabalhadores ativos, mas também ex-trabalhadores e candidatos a um emprego, uma vez que o tratamento de dados pessoais tem consequências para essas três categorias de trabalhadores. Assim, por exemplo, o tratamento de dados não termina necessariamente quando cessa a relação de trabalho. Os empregadores conservam em geral uma parte desses dados, por exemplo, para fornecer provas de que empregaram uma determinada pessoa durante um certo período ou para fornecer informações sobre ex-trabalhadores. Além disso, durante os períodos de recrutamento, os empregadores conservam e usam dados referentes aos candidatos a emprego.[110] (OIT, 1997, p. 11, tradução nossa).

Além destas duas normativas próprias para o setor empregatício, que tecem considerações sobre itens relevantes como coleta, conservação, armazenamento, uso e comunicação de dados pessoais dos trabalhadores, destaca-se que o RGPD, atento à peculiaridade do tratamento de dados no contexto laboral, autoriza em seu artigo 88 que os Estados-membros ou as convenções coletivas estabeleçam regras específicas para o tratamento dos dados pessoais dos trabalhadores[111] nos seguintes termos:

> 1. Os Estados-Membros podem estabelecer, no seu ordenamento jurídico ou em convenções coletivas, normas mais específicas para garantir a defesa dos direitos e liberdades no que respeita ao tratamento de dados pessoais dos trabalhadores no contexto laboral, nomeadamente para efeitos de recrutamento, execução do contrato de trabalho, incluindo o cumprimento das obrigações previstas no ordenamento jurídico ou em convenções coletivas, de gestão, planejamento e organização do trabalho, de igualdade e diversidade no local de trabalho, de saúde e segurança no trabalho, de proteção dos bens do empregador ou do cliente e para efeitos do exercício e gozo, individual ou coletivo, dos direitos e benefícios relacionados com o emprego, bem como para efeitos de cessação da relação de trabalho.
> 2. As normas referidas incluem medidas adequadas e específicas para salvaguardar a dignidade, os interesses legítimos e os direitos fundamentais do titular dos dados, com especial relevo para a transparência do tratamento de dados, a transferência de dados pessoais num grupo empresarial ou num

---

[110] *En el repertorio se define este término en tanto abarca no sólo los trabajadores en actividad, sino también ex trabajadores y candidatos a un empleo, ya que el tratamiento de datos personales tiene consecuencias para estas tres categorías de trabajadores. Así, por ejemplo, el tratamiento de datos no termina necesariamente cuando cesa la relación de trabajo. Los empleadores conservan en general una parte de estos datos, por ejemplo para aportar pruebas de que han empleado a una determinada persona durante un cierto período o para suministrar información respecto de ex trabajadores. Asimismo, durante los períodos de reclutamiento, los empleadores conservan y utilizan datos referidos a los candidatos de empleo*.

[111] Na visão de Giménez (2019), há uma contradição no RGPD, isso porque, embora o legislador europeu tenha dado importância à proteção de dados pessoais, aprovando o RGPD, verifica-se uma baixa profundidade no que tange a esta proteção no âmbito laboral. Prova disso é que o RGPD deixa aos Estados e aos acordos da empresa o estabelecimento de regras específicas sobre proteção de dados no local de trabalho. Para o autor, esta ampla margem de atuação pode provocar certa insegurança jurídica na empresa em relação ao tratamento de dados pessoais dos trabalhadores.

> grupo de empresas envolvidas numa atividade económica conjunta e os sistemas de controlo no local de trabalho. (UNIÃO EUROPEIA, 2016).

Portanto, além de respeitar as recomendações em matéria de proteção de dados na relação de trabalho, a empresa deve levar em conta que o RGPD não será o único regulamento a ser observado, na medida em que ele próprio possibilita que especificidades sejam incluídas em convenções coletivas e leis nacionais.

Assim, um dos aspectos em que o RGPD incidirá no âmbito das empresas diz respeito à mudança de enfoque sobre a proteção dos dados, o que afetará as relações entre empregador e trabalhadores, a fim de que aqueles estabeleçam uma estrutura segura no processamento dos dados pessoais. Para o atingimento de tal objetivo, as empresas, responsáveis pelo tratamento, precisarão se adaptar, até mesmo em termos de organização e funcionamento, especialmente por meio da criação de uma cultura de tutela dos dados.[112]

Por fim, feitos esses breves apontamentos acerca do sistema protetivo dos dados pessoais e sensíveis no sistema europeu, passando pelo campo laboral com as Recomendações introduzidas pela Organização Internacional do Trabalho, e pelo próprio RGPD, encaminha-se, agora, para o estudo dos dados pessoais e sensíveis no âmbito nacional.

3.2 OS DADOS PESSOAIS E SENSÍVEIS NO ORDENAMENTO JURÍDICO BRASILEIRO

No Brasil, a preocupação quanto à proteção dos dados pessoais e sensíveis é recente. A Constituição Federal de 1988 não previu expressamente este direito. Contudo, vários juristas, dentre eles, Têmis Limberger (2009), Danilo Doneda (2011), Júlio Ricardo de Paula Amaral (2015) e Ricardo Villas Bôas Cueva (2017), sustentam que os direitos fundamentais nela previstos representaram a introdução dessa proteção no ordenamento brasileiro.

Nesse sentido, destaca-se o artigo 5º, *caput* e inciso X, que dispõem sobre as garantias constitucionais da liberdade, da privacidade, da intimidade, da vida privada, bem como do livre desenvolvimento da personalidade da pessoa natural, o inciso XII, o qual estabelece uma proteção genérica ao sigilo dos dados, e o inciso

---

[112] Remete-se o leitor ao capítulo 4 para maior aprofundamento do tema.

LXXII, que prevê o *habeas data*, remédio constitucional específico para proteger os dados do cidadão mantidos pelo Estado[113].

Portanto, a partir deste conjunto de dispositivos é possível extrair, ainda que de modo incipiente, o fundamento normativo constitucional para a proteção de dados pessoais. Com relação ao tema, parte da doutrina e da jurisprudência:

> [...] reconhecem que o direito à privacidade abrange, hoje, não apenas a proteção à vida íntima do indivíduo, mas também a proteção de seus dados pessoais, alcançando qualquer ambiente onde circulem dados do seu titular, sendo certo que tais dados, longe de representarem "informações sem dono" livremente coletáveis na internet, exprimem uma abrangente projeção da personalidade humana, exigindo firme proteção da ordem jurídica. (SCHREIBER, 2018).

Além disso, verifica-se que a própria noção de privacidade se amplia, superando a perspectiva meramente individualista para adquirir um valor social. Ou seja:

> [...] a privacidade é encarada como um *bem comum*, que detém particular importância para o estado democrático de direito, por garantir uma participação deliberativa e heterogênea entre os cidadãos em contraste às sociedades totalitárias. A privacidade não beneficia, portanto, somente o indivíduo, mas, colateralmente, a sociedade, revelando-se como um elemento constitutivo da própria vida em sociedade.

---

[113] O habeas data (artigo 5º, LXXII, da CF) destina-se basicamente a possibilitar o direito de acesso e retificação dos dados pessoais. Foi introduzido pela Constituição de 1988 como "um instrumento para a requisição das informações pessoais em posse do poder público, em particular dos órgãos responsáveis pela repressão durante o regime militar e sem maiores vínculos, portanto, com uma eventual influência da experiência europeia ou norte-americana relativa à proteção de dados pessoais, já em pleno desenvolvimento à época. Posteriormente o *habeas data* foi regulamentado pela Lei 9.507, de 1997. A ação de *habeas data* visa a assegurar um direito presente em nosso ordenamento jurídico, ainda que não expresso literalmente. Por meio dela, o cidadão pode acessar e retificar seus dados pessoais em bancos de dados "de entidades governamentais ou de caráter público" (posteriormente ampliou-se o sentido deste "caráter público", incluindo-se os bancos de dados referentes a consumidores, mesmo que administrados por privados). A ação não é acompanhada, porém, de instrumentos que possam torná-la ágil e eficaz o suficiente para a garantia fundamental de proteção dos dados pessoais: além do seu perfil estar demasiadamente associado à proteção de liberdades negativas, algo que se percebe em vários dos seus pontos estruturais, como a necessidade de sua interposição por meio de advogado ou então a necessidade de demonstração de recusa de fornecimento dos dados por parte do administrador de banco de dados, ela é, substancialmente, um instrumento que proporciona uma tutela completamente anacrônica e ineficaz à realidade das comunicações e tratamentos de dados pessoais na Sociedade da Informação." (DONEDA, 2011, p. 104). Como reflexo desta ineficácia, Cachapuz (2014, p. 831) aponta que "Na prática jurisprudencial, a previsão constitucional tem se traduzido antes como um norte jurídico – de prerrogativa constitucional relativa ao acesso a informações nominativas –, do que propriamente como um efetivo instrumento de uso forense para a defesa de interesses privados. Nos tribunais, a defesa do direito de acesso tem sido postulada, com frequência, por meio de tutelas inibitórias mais amplas, que abranjam, cumulativamente, a possibilidade indenizatória em face de prejuízo demonstrado em concreto – situação inatingível por meio de um remédio constitucional."

> O relato normativo da privacidade contextual capta essa mensagem e a verticatiza para a proteção de dados pessoais, na medida em que se propõe a investigar quais são as implicações do fluxo informacional para as interações sociais. (BIONI, 2019, p. 216).

Na esfera infraconstitucional, em 1990, o Código de Defesa do Consumidor (CDC) garantiu o direito de acesso e retificação de dados nos artigos 43 e 44, estabelecendo regras específicas sobre banco de dados e cadastros de consumidores. Embora pioneiras, as medidas previstas pelo CDC restringem-se a situações em que os dados em questão pertencem a consumidores, além do que são ações que não asseguram uma tutela integral da privacidade.

Posteriormente, implementou-se a Lei de Sigilo Bancário[114] para orientar a proteção de dados acerca de operações financeiras. A preocupação pontual do legislador com o direito à proteção de dados também esteve presente na Lei do Cadastro Positivo[115] e na Lei de Acesso à Informação[116]. Após, em 23 de abril de 2014, foi instituído pela Lei nº 12.965 o Marco Civil da Internet, cuja proteção aos dados pessoais constou em seu artigo 3º, inciso III, como um de seus princípios. Dessa forma:

> [...] até a entrada em vigor do Marco Civil da Internet em 2014, os dados do usuário estiveram protegidos apenas em relações jurídicas específicas, abordadas por legislações esparsas. No entanto, nem mesmo o Marco Civil tratou do direito à proteção de dados de maneira exaustiva, função que coube à Lei Geral de Proteção de Dados. [...] Há uma lacuna temporal entre a chegada da internet no Brasil e o Marco Civil da Internet como uma lei mais específica, ainda que não completamente satisfatória, para regular a proteção de dados de usuários da internet: a internet foi trazida para o Brasil em meados de 1990, enquanto a lei que estabelecia os princípios, garantias e direitos para o uso da internet só apareceu em 2014, mais de vinte e cinco anos depois. (BRITTO; RIBEIRO, 2018, p. 389).

O Código Civil, por sua vez, limitou-se a repetir em seu artigo 21, disposição acerca da proteção da privacidade já prevista na Constituição Federal, sem estipular nenhuma proteção acerca dos dados pessoais.

Verifica-se, portanto, até então, a ausência de uma norma específica acerca do direito à proteção de dados pessoais, o qual “encontrava uma tutela

---

[114] Lei Complementar nº 105, de 10 de janeiro de 2001.
[115] Lei nº 12.414, de 9 de junho de 2011.
[116] Lei nº 12.527, de 18 de novembro de 2011.

meramente reflexa em nossa legislação, sendo tangenciado por leis esparsas."[117] (SCHREIBER, 2018). Assim, o ordenamento jurídico brasileiro carecia de instrumentos legais que assegurassem uma tutela jurídica de defesa dos dados pessoais e sensíveis, de modo a harmonizar o desenvolvimento da tecnologia com a preservação dos direitos de personalidade[118] e de privacidade dos seus titulares.

Somente em 2018, inspirado no Regime Geral sobre a Proteção de Dados ou *General Data Protection Regulation*, com incidência no âmbito da União Europeia,[119] o Congresso Nacional Brasileiro aprovou a Lei nº 13.709 de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados (LGPD)[120], com previsão de entrada em vigor em 2020.

Tal "corrida" pela aprovação da LGPD se explica[121], pois, além do atraso legislativo em matéria de proteção de dados e o escândalo de vazamento envolvendo o *Facebook* e a *Cambridge Analytica*[122], o GDPR estabeleceu que empresas europeias somente podem contratar empresas estrangeiras se essas estiverem localizadas em países que possuam grau de proteção igual ou superior ao estabelecido em seu território, o que acabava excluindo o Brasil, causando desvantagem competitiva para as empresas nacionais e sua marginalização no cenário econômico mundial.[123] (OLIVEIRA, 2018).

---

[117] Diante da insuficiência de disposições, coube à doutrina os esforços para a construção sistemática de um direito à proteção de dados pessoais, dotado de uma lógica própria e funcionalizado à tutela da pessoa humana, com destaque para a obra precursora de Danilo Doneda, *Da Privacidade à Proteção de Dados Pessoais*, Rio de Janeiro: Renovar, 2006 e o livro de Laura Schertel Mendes*, Privacidade, Proteção de Dados e Defesa do Consumidor*, São Paulo: Saraiva, 2014. (SCHREIBER, 2018).

[118] Para Doneda (2006, p. 168), "por força do regime privilegiado de vinculação entre a informação pessoal e a pessoa à qual se refere – como representação direta da personalidade – tal informação deve ser entendida como uma extensão da sua personalidade."

[119] "Embora aplicável formalmente apenas no âmbito da União Europeia, a regra tem, na prática, alcance mundial, em razão da integração global típica da internet e da relevância do bloco europeu no contexto econômico internacional." (SCHREIBER, 2018).

[120] Tal como no Regulamento europeu, o modelo legislativo estabelecido no Brasil apresenta caráter preventivo, o que se denota, por exemplo, nos artigos 6º, II, VI, VII, VIII e X, artigo 46, *caput*, e § 2º, e artigo 47 da LGPD, na medida em que "busca-se antecipar os riscos de violação à privacidade, além de evitar danos à pessoa humana, tratamentos abusivos de informações e vazamentos de dados." (TEPEDINO; TEFFÉ, 2019, p. 293).

[121] Fala-se em "corrida", pois diversos projetos de lei sobre proteção de dados pessoais tramitaram lentamente no Congresso Nacional durante alguns anos, sendo que após os diversos atores sociais envolvidos na matéria (pesquisadores, empresários e representantes da sociedade civil) alcançarem algum consenso, foi possível a aprovação na Câmara dos Deputados do Projeto de Lei nº 4.060/2012, que passou, sem alterações, pelo Senado Federal, e acabou sancionado pelo Presidente Michel Temer em 14 de agosto de 2018. (SCHREIBER, 2018).

[122] Acerca do escândalo envolvendo o *Facebook* e a *Cambridge Analytica* remete-se o leitor ao item 2.3.

[123] De acordo com a Comissão Europeia, até o presente momento, Andorra, Argentina, Canadá (organizações comerciais), Ilhas Faroe, Guernsey, Israel, Ilha de Man, Japão, Jersey, Nova Zelândia,

Dessa maneira, a aprovação da LGPD equiparou o Brasil a outros países considerados adequados para salvaguardar os dados pessoais, representando um avanço na proteção dos direitos fundamentais de seus cidadãos.[124] Nesse sentido, Tepedino e Teffé (2019, p. 288) reforçam que:

> A proteção dos dados pessoais compõe uma das partes essenciais da tutela da dignidade, mostrando-se essencial para a garantia das liberdades fundamentais, da igualdade e da integridade psicofísica. O desenvolvimento de mecanismos destinados a regular o tratamento de dados auxilia a evitar discriminações que não encontrem fundamento constitucional, como aquelas que possam dificultar o acesso ao crédito ou a empregos por determinados grupos. Além disso, afasta práticas que possam reduzir a liberdade e autonomia dos indivíduos, como decisões a partir de análises de dados não informadas ao titular e sob critérios não transparentes. A tutela dos dados relativos à pessoa natural mostra-se hoje vital para que ela se realize integralmente e se relacione na sociedade, representando garantia de maior segurança às informações dos cidadãos e impedindo práticas autoritárias e de vigilância por parte de instituições públicas e privadas.

Assim, a Lei nº 13.709/2018, recentemente aprovada, dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, e tem por objetivo a proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A LGPD, tal qual o RGPD, fixa alguns conceitos, como no artigo 5º, inciso I, ao considerar dado pessoal a "informação relacionada a pessoa natural identificada ou identificável". O parágrafo 2º do artigo 12 também inclui como dados pessoais "aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada." (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

Dentro dos dados pessoais, da mesma forma que no RGPD, há também os chamados dados pessoais sensíveis que, de acordo com o artigo 5º, inciso II, referem-se aos dados:

Suíça, Uruguai e Estados Unidos da América (limitado à estrutura do *Privacy Shield*) são os países reconhecidos por gozarem de um nível adequado de proteção de dados fora do âmbito da União Europeia. (COMISSÃO EUROPEIA, 2019).

[124] Stival (2015) ressalta que a importância da aprovação de uma lei geral de proteção de dados no Brasil se justifica por diversos motivos, dentre eles, pelo fato de haver Juízes de matriz positivista, que defendem que o direito está no texto legal e nada mais. Além disso, a fixação detalhada dos princípios gerais, dos requisitos, dos direitos do titular, das regras para o tratamento de dados pessoais, do estabelecimento de sanções administrativas e de uma autoridade de garantia, trazem maior efetividade e concretizam o direito fundamental extraído da Constituição Cidadã. Nesse sentido, Limberger (2009, p. 47) acrescenta que "toda a legislação, além da proteção intrínseca que traz em si mesma aos direitos, com a possibilidade de aplicação, contém o aspecto pedagógico, no sentido de despertar que os dados pessoais têm uma importância na sociedade atual."

> sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

Outro conceito chave refere-se ao do tratamento de dados, que compreende, nos termos do artigo 5º, inciso X:

> 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. (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

Como se observa, as atividades que abrangem o tratamento de dados são muitas.[125] Em linhas gerais, na dinâmica do *Big Data*[126], os dados são coletados das mais variadas formas, como em transações comerciais, pesquisas de mercado e de estilo de vida, censo de registros e interações em meios digitais. O armazenamento se dá em enormes bancos de dados. O processamento, por sua vez, consiste em técnicas de análise e refinamento dos dados, com o intuito de deles extrair informações úteis e valiosas. Por fim, a difusão está associada à ideia de mercado de dados pessoais, que pode ser entendida como interações econômicas voltadas à compra e venda de informações.

No que tange à aplicação da LGPD, esta possui eficácia extraterritorial, na medida que, consoante o artigo 3º, incide sobre:

---

[125] Só no contexto laboral, inúmeras são as situações que envolvem o fluxo de dados pessoais dos trabalhadores. Menciona-se desde a fase anterior à celebração do contrato (recrutamento de pessoal, candidaturas espontâneas, informações sobre o candidato, avaliação de currículo, histórico, dentre outras), passando pela fase de celebração do contrato (acesso a dados cadastrais, filiação a sindicado, endereço, nomes dos genitores, escolaridade, situação familiar, nomes dos filhos, idade, tipo sanguíneo, dentre outras) e, ainda a fase de execução do contrato de trabalho (jornada de trabalho, valor do salário, descontos, faltas, motivos das faltas, doenças, acidentes, situações conjugais, que podem ter reflexos na empresa, como o pagamento de pensão, inclusão de um dependente no plano de saúde, procedimentos disciplinares, comunicações entre trabalhadores e empregador, *profiling* – avaliação de desempenho, dentre outras) e, por fim, a fase do término do contrato de trabalho (motivo do desligamento, valor das verbas rescisórias, entre outras). Há, ainda, as situações que envolvem troca de informações entre o empregador e terceiros (sindicatos, outras empresas, inclusive terceirizadas, órgãos públicos, empresas de planos de saúde, consultorias contratadas, dentre outras).

[126] Para maior aprofundamento sobre o *Big Data*, remete-se o leitor ao item 2.1.

> 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; 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. § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta. § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei[127]. (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

Quanto aos sujeitos abrangidos, a LGPD considera titular a "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento"[128]. Além deste, a lei disciplina os agentes de tratamento, que se dividem nas figuras do controlador e do operador, os quais correspondem à pessoa natural ou jurídica, de direito público ou privado, sendo que, ao controlador, nos termos do inciso VI, "competem as decisões referentes ao tratamento de dados pessoais" e, ao operador, nos termos do inciso VII, cabe realizar o tratamento de dados pessoais em nome daquele.[129] (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

Assim, uma vez identificado o titular dos dados pessoais, o artigo 18 da LGPD estabelece um rol de direitos a serem exercidos, a qualquer momento e mediante requisição, em face do controlador.[130]

Nessa perspectiva, o titular dos dados pessoais tem direito à *confirmação da existência de tratamento*, o *acesso aos dados*, a *correção de dados incompletos, inexatos ou desatualizados*, a *anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD*, *a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição*

---

[127] O inciso IV do *caput* do art. 4º prevê que: "Esta Lei não se aplica ao tratamento de dados pessoais: 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. (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

[128] Inciso V do artigo 5º da Lei nº 13.709, de 14 de agosto de 2018.

[129] No ambiente laboral, diante do exposto, resulta que os empregadores são sujeitos regulados pela LGPD, uma vez que na condição de pessoa física ou jurídica, coletam e armazenam dados pessoais, seja para uso exclusivamente pessoal, seja para cumprir obrigação em matéria de seguridade social e tributária, por exemplo.

[130] Quanto a este aspecto, importante referir que a "LGPD representa a consolidação de relevante paradigma: atribuir a titularidade dos dados à pessoa natural a eles referente, conferindo-lhe extensa miríade de direitos para empreender efetivo controle sobre as suas informações." (FRAZÃO; OLIVA; ABILIO, 2019, p. 693).

expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial, a *eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da LGPD*[131]*,* a *informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados*; a *informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa* e a *revogação do consentimento*.

Dentre os mencionados direitos, ressalta-se a anonimização e o direito ao esquecimento, por serem direitos não tão difundidos.

A anonimização de dados pessoais consiste na "retirada do vínculo da informação com a pessoa a qual se refere – é um recurso que algumas leis de proteção utilizam para diminuir os riscos presentes no seu tratamento" (DONEDA, 2006, 157-158). A LGPD prevê esta possibilidade no seu artigo 5º, inciso XI.[132] Trata-se de um "mecanismo capaz de auxiliar o uso eficiente e seguro do *Big Data*. [...] A aproximação impede que o uso da informação possibilite a verificação da identidade individual do titular." (CAVALCANTI; SANTOS, 2018. p. 360).

Ao lado da anonimização, a LGPD estabelece a chamada pseudonimização[133] no artigo 13, § 4º.[134] Ambas devem ser observadas, sempre que possível, na realização de estudos na área de saúde pública por órgãos de pesquisa. Além disso, a utilização do dado anônimo também pode ser útil ao possibilitar a "comunicação e expressão de sujeitos que estariam impedidos, por vínculos e

---

[131] Conforme o artigo 16 da LGPD: "Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: I – cumprimento de obrigação legal ou regulatória pelo controlador; II – estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; III – transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou IV – uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados." (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

[132] A anonimização consiste na "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." (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

[133] A pseudonimização corresponde 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." (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

[134] O Parecer 05/2014 sobre técnicas de anonimização do Grupo de Trabalho sobre Proteção de Dados do Artigo 29 (GT29, 2014a) elenca uma serie de técnicas que as empresas podem incorporar em sua organização, como a cifragem com chave secreta e a utilização de dispositivos de autenticação (*tokens*), dentre outras, as quais podem ser utilizadas para garantir a segurança dos dados pessoais dos trabalhadores que enfrentam interferência de terceiros. Giménez (2019) indica que a incorporação de algumas dessas medidas implicaria uma redução nos riscos para as partes interessadas, além de auxiliar os agentes de tratamento no cumprimento das obrigações de proteção de dados.

limitações políticas ou sociais, de exprimir-se livremente", como aponta Doneda (2006, p. 158).

Já o direito ao apagamento dos dados, também conhecido como "direito ao esquecimento" ou "direito a ser esquecido", previsto no artigo 17 do RGPD, consiste no direito que o titular tem de obter do responsável pelo tratamento o apagamento dos seus dados pessoais em algumas situações, entre elas, quando deixarem de ser necessários para a finalidade que motivou o seu recolhimento, quando o consentimento para o tratamento for retirado ou, ainda, quando os dados forem tratados ilicitamente.

No Brasil, a LGPD, embora não utilize a mesma nomenclatura, determina, em seu artigo 16, a eliminação dos dados pessoais após o término de seu tratamento em razão de a finalidade ter sido alcançada, de os dados deixaram de ser necessários ou pertinentes ao alcance do objetivo almejado ou pela revogação do consentimento, conforme dispõe o artigo 15. Todavia, relevante notar que:

> Tais hipóteses, a rigor, não configuram consagrações legais do que se tem denominado *direito ao esquecimento*, que, apesar do nome, deve ser compreendido de modo mais estrito, como o direito de cada pessoa humana de se opor à recordação opressiva de determinados fatos perante a sociedade, que lhe impeça de desenvolver plenamente sua identidade pessoal, por enfatizar perante terceiros aspectos de sua personalidade que não mais refletem a realidade. (SCHREIBER, 2018).

Ainda quanto à LGPD, é preciso atentar que a referida lei foi elaborada visando assegurar uma proteção aos dados pessoais dos consumidores, sem previsão regulatória no tocante aos dados pessoais dos trabalhadores,[135] os quais, pela condição de vulnerabilidade e hipossuficiência, podem encontrar dificuldades quanto ao pleno exercício de alguns direitos relacionados ao tratamento dos seus dados. Assim, diante das especificidades da relação laboral:

> Não seria exagero, inclusive, a postulação de uma regulamentação posterior específica para a proteção dos dados pessoais dos trabalhadores. A recorrência a um método regulatório setorial seria o reconhecimento de que as relações de trabalho são diferentes das relações comerciais, as quais o anteprojeto de lei de proteção de dados pátrio visa efetivamente normatizar. (STIVAL, 2015, p. 143).

[135] Da mesma forma, como visto no tópico anterior, o RGPD também não se aprofunda na questão envolvendo o tratamento de dados nas relações de trabalho.

Não obstante, enquanto não sobrevém este marco regulatório específico, é possível se trabalhar com a noção do chamado “microssistema jurídico de direitos da personalidade do trabalhador”, defendida por Goldschmidt (2019b), para lhe assegurar a proteção aos dados pessoais e sensíveis. Nesse sentido, a partir dos ensinamentos do referido autor, o novel artigo 223-C da CLT[136] elenca, de forma meramente exemplificativa, bens extrapatrimoniais do trabalhador, tuteláveis juridicamente.

Diante disso, muito embora o dispositivo preveja expressamente a intimidade, não fecha a porta para outros bens, entre eles, especificamente os dados pessoais e sensíveis, considerado como um direito de personalidade da pessoa-trabalhadora.[137]

À vista disso, uma vez que os dados pessoais e sensíveis refletem uma das múltiplas expressões da personalidade do trabalhador no âmbito das relações trabalhistas, fundamental que se construa um “sistema de promoção e defesa” desses dados.

Nessa perspectiva, para garantir tal defesa, Carvalho (2019, p. 228), propõe a adoção da denominada tutela específica[138], prevista no artigo 12 do Código Civil[139], “enquanto resposta adequada para a proteção dos direitos da personalidade do trabalhador[140], em oposição à mera condenação ao pagamento de indenização pelos danos eventualmente verificados.”

Como observa o autor (2019), em se tratando de direitos de personalidade, a noção de tutela específica é ainda mais relevante, na medida em que:

---

[136] “Art. 223-C. A honra, a imagem, a intimidade, a liberdade de ação, a autoestima, a sexualidade, a saúde, o lazer e a integridade física são os bens juridicamente tutelados inerentes à pessoa física.” (BRASIL. Decreto-Lei nº 5.452, de 1º de maio de 1943).

[137] Sobre o tema, remete-se o leitor ao item 3.4, no qual se discorre sobre a proteção dos dados pessoais e sensíveis como direito fundamental do trabalhador.

[138] Segundo Carvalho (2019, p. 231), a tutela específica do direito material “é aquela que está preocupada com a integralidade do direito, não se conformando com a mera conversão no equivalente monetário ao bem lesado. A tutela específica busca, ao final do processo, produzir resultado que coincida com o conteúdo do direito material.”

[139] “Art. 12. Pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei.” (BRASIL. Lei 10.406, de 10 de janeiro de 2002).

[140] Ao lado do artigo 12 do Código Civil, Carvalho (2019) acrescenta mais dois dispositivos: o artigo 21 do mesmo diploma, o qual complementa a ideia de que, diante de ato contrário a direito de personalidade, o juiz adotará as providências necessárias para impedi-lo ou fazê-lo cessar, e o artigo 499 do Código de Processo Civil, que também traz comando que prioriza a tutela específica (ou a obtenção da tutela pelo resultado prático equivalente).

> [...] a tutela ressarcitória clássica (ou seja, o pagamento de quantia equivalente após a violação do direito) não se revela a maneira mais adequada para a proteção dos direitos da personalidade, tão ligados à própria dignidade da pessoa humana, e que não podem se dar ao luxo de aguardar eventual violação para, só então, desfrutarem de algum tipo de tutela.
> [...]
> Afinal, garantir o direito à tutela ressarcitória (indenização) não é tão eficiente quanto promover a tutela específica diante de violação a direitos de personalidade. A tutela ressarcitória parte da premissa de que o dano já ocorreu. Já a tutela específica pode até mesmo impedir a ocorrência da violação ao direito. (CARVALHO, 2019, p. 232).

Portanto, como mencionado, a LGPD estabelece em seu artigo 18 um rol de direitos ao titular dos dados e, o artigo 22, ainda prevê de forma expressa a possibilidade de defesa em juízo dos interesses e dos direitos dos titulares de dados, seja de forma individual ou coletiva.[141]

Apesar disso, dada a peculiaridade da relação de trabalho, a questão que se coloca é se esse rol de direitos estabelecidos ao titular dos dados (posição ocupada pelo trabalhador) serão exercidos da maneira desejada, visto que do outro lado, o agente de tratamento é o empregador.

Em razão do exposto, no que tange ao exercício dos direitos de confirmação da existência de tratamento de dados, de acesso, de retificação[142] e cancelamento de dados pessoais do trabalhador, para evitar que tais direitos fiquem inoperantes, Stival (2015) trabalha com a sugestão da Professora Susana Rodríguez Escanciano, em sua obra '*El derecho a la protección de los datos personales de los trabajadores: nuevas perspectivas*', denominada "direito de acesso passivo", que "consiste na exposição dos dados, pelo detentor destes, de quando em quando, de ofício, ao empregado, e sempre que acontecer modificações e cessões a terceiros."[143]

---

[141] Menciona-se aqui a possibilidade de o Ministério Público do Trabalho, enquanto Órgão responsável pela defesa da ordem jurídica e dos direitos sociais, difusos, coletivos, individuais homogêneos, atuar na tutela dos dados pessoais dos trabalhadores.

[142] Com relação a este direito, o Repertório de Recomendações Práticas da OIT (OIT, 1997) prevê que se o empregador se recusar a retificar os dados pessoais, o trabalhador deve ter direito a incluir ou adicionar em seu expediente uma nota indicando as razões da sua discordância, a qual deverá estar presente em toda utilização subsequente dos dados pessoais, assim como deverá constar que estes foram contestados.

[143] Dada a peculiaridade da relação laboral, em que as partes encontram-se em posições desiguais, outra medida a ser adotada para proteger os dados pessoais e sensíveis do trabalhador de uma possível lesão (ou ameaça), seria o manejo da tutela específica, como proposto por Carvalho (2019). No caso, a depender do ato ilícito praticado pelo agente de tratamento (empregador), caberá o ajuizamento da chamada 'tutela inibitória' (a qual busca inibir a prática, a reiteração ou continuação do ato) ou ainda da chamada 'tutela de remoção do ilícito' (a qual visa remover a causa ou os efeitos do ilícito). Salienta-se que tais tutelas podem ser buscadas até mesmo por meio da ação civil pública, sendo que o manejo pela via coletiva resulta em duplo benefício à pessoa-trabalhadora: impede que os direitos previstos na LGPD fiquem inoperantes, podendo inclusive incidir *astreintes* em caso de

Trata-se de medida que “permitiria o acesso indiscriminado de todos os trabalhadores a todos os seus dados pessoais sem a necessidade de exposição que causasse qualquer desconforto aos titulares dos dados.” (STIVAL, 2015, p. 134).

Outro ponto que merece destaque é o consentimento do titular dos dados, enquanto requisito para a promoção do tratamento, previsto no artigo 5º, XII, da Lei nº 13.709/2018[144]. Tal instituto tem “importante papel na autodeterminação informativa, controle e liberdade do titular em relação aos seus dados, configurando-se elemento central para a proteção de dados pessoais.”[145] (CAVALCANTI; SANTOS, 2018. p. 359).

Porém, há situações em que o consentimento não pode servir como único elemento legitimador para o tratamento de dados pessoais e sensíveis. Acerca do tema, o Grupo de Trabalho do artigo 29º para a Proteção de Dados – GT29, criado pela Diretiva 95/46/CE do Parlamento Europeu e do Conselho da União Europeia[146], de 24 de outubro de 1995, ao discutir sobre os elementos do consentimento válido nos casos envolvendo relação laboral, assinalou que em razão da dependência existente entre empregador e trabalhador:

> é improvável que o titular dos dados possa recusar ao seu empregador o consentimento para o tratamento dos dados sem que haja medo ou risco real de consequências negativas decorrentes da recusa. É improvável que um trabalhador responda livremente ao pedido de consentimento do empregador para, por exemplo, ativar sistemas de controlo como a observação do local de trabalho através de câmaras ou preencher formulários de avaliação, sem sentir qualquer tipo de pressão para dar esse consentimento. (GT29, 2018).

Portanto, o GT29 da OIT considera que o fundamento legal para o tratamento de dados pessoais e sensíveis dos trabalhadores atuais ou futuros não

---

desobediência à decisão e, como o exercício da tutela não ocorre pela via individual, afastam-se possíveis perseguições ou retaliações por parte do empregador.

[144] O consentimento consiste na “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.” (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

[145] A propósito da noção de consentimento, Tepedino e Teffé (2019, p. 291) observam que este vem passando por uma evolução “do consentimento implícito (situação em que se entende que uma pessoa consentiu com algo em razão da conduta que assume) para o consentimento informado, o qual orienta inclusive normas relativas à circulação de informações. [...] No momento atual, o consentimento informado vem ganhando cada vez mais prestígio, por tornar o usuário participante ativo no processo de consentimento.”

[146] Trata-se de um órgão consultivo europeu independente em matéria de proteção de dados e privacidade. As suas atribuições encontram-se descritas no artigo 30º da Diretiva 95/46/CE e no artigo 15º da Diretiva 2002/58/CE. Cabe, porém, mencionar que com a aprovação do RGPD ficou estabelecido que caberá ao Comitê Europeu substituir o Grupo de Trabalho sobre a proteção das pessoas a fim de promover a aplicação coerente do regulamento. (UNIÃO EUROPEIA, 2016).

pode nem deve ser o consentimento, dada a natureza da relação laboral, “sob pena de se acabar autorizando situações de verdadeira e inadmissível renúncia de direitos.”[147] (STIVAL, 2015, p. 129). Corroborando esse entendimento, Novais (2016) aponta para a existência de limites e alerta que nem sempre o consentimento salva de invalidade jurídica a correspondente ação ou omissão. Ou seja:

> haverá situações em que o próprio consente, no sentido de que aceita ou promove agressões em bens e direitos vitais da sua esfera pessoal, e ainda assim, esse consentimento livremente estabelecido não deve ser juridicamente reconhecido por força do necessário respeito da dignidade da pessoa humana. (NOVAIS, 2016, p. 141).

Contudo, apenas para encerrar a questão do consentimento, embora na maior parte do tratamento de dados no local de trabalho o fundamento legal não possa ser o consentimento dos trabalhadores, o próprio GT29 da OIT reconhece que isso não significa que os empregadores nunca possam utilizá-lo como fundamento legal para o tratamento. Poderá haver situações em que seja possível ao empregador demonstrar que o consentimento foi dado livremente, ou seja, em circunstâncias excepcionais, quando o ato de dar ou recusar o consentimento não produzir quaisquer consequências negativas.[148]

Voltando à questão da proteção de dados e a sua incidência nas relações de trabalho frente às novas tecnologias, o tema, embora ainda de modo incipiente, tem despertado preocupações e discussões entre os membros que atuam na área trabalhista do Judiciário Brasileiro. Conforme se verifica, nas últimas edições dos

---

[147] Ainda, no ponto, não se pode esquecer do teor do artigo 468 da CLT, segundo o qual só é lícita a alteração das condições contratuais de trabalho, o que abrange o eventual tratamento de dados, com o mútuo consentimento e, desde que, não resulte prejuízos diretos ou indiretos ao empregado, justamente para lhe proteger da condição de hipossuficiência e vulnerabilidade em face do seu empregador. Segundo a doutrina, trata-se do chamado ‘princípio da inalterabilidade contratual lesiva’ (DELGADO, 2017). Também, o dispositivo em comento dá roupagem normativa para aquilo que a doutrina chama de “proteção da boa-fé objetiva” (a qual no contrato de trabalho pressupõe uma conduta dos sujeitos fundada na lealdade, na confiança e na colaboração), além de glosar o eventual “abuso de direito” por parte do empregador. Nesse sentido, como observa Nascimento (2011), a boa-fé constitui um dos suportes do contratualismo contemporâneo, a qual põe-se numa diretriz limitativa da liberdade contratual e também como forma de corrigir os desvirtuamentos e o abuso de direito existentes contratos de trabalho.

[148] Nesse sentido, o GT29 da OIT exemplifica a seguinte situação: “Uma equipa de filmagem pretende filmar determinada parte de um escritório. O empregador solicita o consentimento de todos os trabalhadores que se sentam nessa zona do escritório para serem filmados, uma vez que podem aparecer em segundo plano nas filmagens do vídeo. Os trabalhadores que não quiserem ser filmados não serão de forma alguma penalizados, uma vez que serão colocados noutro local de trabalho equivalente numa outra zona do edifício enquanto durar a filmagem.” (GT29, 2018).

Congressos Nacionais dos Magistrados do Trabalho (CONAMAT) foram apresentadas algumas teses sobre o assunto.

Em 2008, durante o XIV CONAMAT, foi apresentada a seguinte tese:

> **XIV CONAMAT (2008) – COMISSÃO 1 – AS NOVAS TECNOLOGIAS E AS RELAÇÕES DE TRABALHO** Tese 2: Os bancos informatizados de dados permitem traçar o perfil ideológico, racial, sexual ou psicológico do trabalhador, podendo vulnerar o direito à intimidade ou ensejar práticas discriminatórias na empresa. O direito à intimidade informática do trabalhador está fundado nos princípios da finalidade e autodeterminação informativa. O primeiro impõe a conexão entre a informação cadastrada e um interesse empresarial legítimo, e o segundo pressupõe o consentimento inequívoco do trabalhador e a possibilidade de vindicar a alteração de dados, quando errôneos ou desatualizados. (ANAMATRA, 2015, p. 154).

De fato, como abordado no capítulo anterior, a elaboração de perfis propiciada pela economia baseada no processamento de dados torna-se cada vem mais presente no ambiente laboral, permitindo ao empregador descobrir, a partir das informações disponibilizadas, aspectos relacionados à personalidade do trabalhador, suas preferências, gostos, interesses, amizades, dentre outras.

Ocorre que muitas destas informações acabam sendo coletadas pelas empresas de forma abusiva, sem guardar qualquer relação com os princípios fundamentais de tratamento de dados e a sua correspondente aplicação na relação de trabalho, ensejando, muitas vezes, além da violação aos dados e à vida privada do trabalhador, práticas discriminatórias, tal como a conduzida pela empresa *Amazon.com*[149], como se todas as ações estivessem amparadas pelo legítimo interesse empresarial.[150]

Em 2010, no XV CONAMAT, foi apresentada a seguinte tese:

> **XV CONAMAT (2010) – COMISSÃO 4 – PROCESSO VIRTUAL: TENSÕES ENTRE A EFICIÊNCIA E O EXERCÍCIO DE DIREITOS FUNDAMENTAIS** Tese 1) AGLUTINADA O PROCESSO ELETRÔNICO E O RISCO DE DADOS SENSÍVEIS: A adoção do processo eletrônico não pode violar a proteção aos dados sensíveis dos trabalhadores, incluindo-se aí a informação sobre a existência do próprio processo trabalhista. Todo e qualquer meio de discriminação não poderá ser permitida pela hiperexposição de dados sensíveis. (ANAMATRA, 2015, p. 184).[151]

---

[149] Remete-se o leitor ao item 2.4, no qual se elucida o caso da empresa *Amazon.com* com maiores detalhes.

[150] O tema do legítimo interesse será melhor desenvolvido no item 4.1.

[151] Menciona-se que no ano de 2014, o Conselho Superior da Justiça do Trabalho, preocupado com a divulgação de dados processuais eletrônicos na rede mundial de computadores, publicou a Resolução nº 139, que dispõe sobre medidas a serem adotadas pelos Tribunais Regionais do Trabalho para

Acerca da publicação de decisões nos portais dos Tribunais trabalhistas e a vulnerabilidade dos dados pessoais dos empregados, as NTIC têm ultrapassado o processo eletrônico e abarcado a divulgação das decisões jurisdicionais nos portais institucionais, o que tem ensejado riscos:

> [...] sobretudo quando são expostos dados pessoais e informações de caráter íntimo das partes envolvidas no processo, fato que viola a intimidade e tem potencial para gerar discriminação e preconceito. Essa situação assume ainda maior relevância quando os dados divulgados são de empregados que procuraram o Poder Judiciário para reclamar direitos trabalhistas não satisfeitos, cuja decisão posteriormente divulgada pode dificultar, senão impedir, seu acesso a novos postos de emprego." (SILVA, 2019, p. 152).[152]

E, em 2012, da XVI CONAMAT sobreveio a seguinte orientação:

> **XVI CONAMAT (2012) – COMISSÃO 1 – NOVAS CONFIGURAÇÕES SOCIAIS E A EFETIVIDADE DA ATIVIDADE JUDICIAL** Tese 7) DADOS PESSOAIS E SENSÍVEIS DO TRABALHADOR. USO E TRATAMENTO. VEDAÇÃO: Os dados pessoais do trabalhador e aqueles sensíveis, referentes às opções religiosa, sexual, filosófica, partidária, entre outras, são protegidos constitucionalmente (art. 5º, incs. X e XII) e por lei (art. 43 do CDC e Lei nº 12.414/2011, aplicados analogicamente ao Direito do Trabalho). Por isso, em regra, não podem ser usados nem tratados sem o consentimento do trabalhador, para fins diversos aos que se destinam. (ANAMATRA, 2015. p. 196).

Ou seja, já no ano de 2012 se reconhecia à pessoa-trabalhadora a titularidade dos seus dados pessoais e sensíveis e a necessidade, a partir das normativas existentes, de tutelar o seu direito fundamental à proteção dos dados.

Acerca do tema, como mencionado, em 2018 foi aprovada a LGPD. Embora não haja previsão expressa nesta normativa quanto à pessoa do trabalhador,

---

impedir ou dificultar a busca de nome de empregados com o fim de elaboração de "listas sujas". (DEJT, 2014).

[152] Com relação a esta hiperexposição, transcreve-se algumas situações relatadas por Silva (2019) em que se verifica a vulneração dos dados pessoais dos jurisdicionados: "ainda que o buscador utilizado no site do Poder Judiciário não permita a localização pela simples digitação do nome da parte, basta lançar o nome da pessoa no Google que este remete para outros aplicativos, a exemplo do Escavador, lá constando referência às ações em que a pessoa eventualmente é parte. Certamente esse registro já aponta para a existência de demandas judiciais, o que estigmatiza o empregado e poderá servir de elemento ainda mais violador, pois basta aprofundar a busca para chegar a dados sensíveis do obreiro, como doenças, orientação sexual, dentre outras informações divulgadas na decisão judicial." Portanto, o que se observa é que, ainda que exista "um padrão mínimo de proteção no qual os motores de busca não poderiam localizar a decisão tão somente pelo nome do jurisdicionado, [...] em casos de ações trabalhistas, o fato é que o inteiro teor das decisões judiciais contém dados pessoais e inúmeras outras informações sensíveis ao titular, e o Estado as divulga sem lhes consultar previamente, o que impede o exercício da autodeterminação informativa." (SILVA, 2019, p. 160-162).

considera-se tal lei aplicável às relações de trabalho. Tal se justifica, primeiro, porque estas relações envolvem tratamento de dados[153] e, segundo, porque inexiste no ordenamento jurídico brasileiro regras específicas dando tratamento detalhado e adequado à proteção de dados pessoais e sensíveis do trabalhador no âmbito das relações de trabalho.

Nesse contexto, inegável que os dados pessoais e sensíveis dos trabalhadores precisam de proteção. Contudo, enquanto não sobrevém uma regulamentação específica, é possível extrair do disposto no artigo 3º da LGPD[154], em conjunto com o disposto no parágrafo 1º do artigo 8º da CLT[155], que a Lei nº 13.709/2018 constitui fonte normativa na proteção aos dados dos trabalhadores.

Nesse sentido, as empresas deverão se adaptar às novas exigências da LGPD, visto que recolhem os mais diversos dados ao longo da relação laboral para atender à determinação da lei, para a realização de processo seletivo, para a formação e aperfeiçoamento de pessoal, para o resguardo da segurança pessoal e laboral, para o controle de qualidade do serviço que prestam aos clientes, para a proteção de seus bens, dentre muitas outras finalidades. Assim, é natural o manejo de dados pessoais e, até mesmo, de dados pessoais sensíveis dos trabalhadores, bem como a sua manutenção durante anos nos bancos de dados[156] da empresa.

---

[153] Como retrata Stival (2015, p. 133-134), são muitas as circunstâncias em que ocorre o tratamento de dados dos trabalhadores: "NO PROCESSO DE OBTENÇÃO DE EMPREGO: para se submeter à seleção, o candidato, muitas vezes, deverá realizar testes, dentre eles o 'psicotécnico', cujos resultados estarão de posse da empresa que está realizando a seleção, que poderá ser, inclusive, terceira e não a empregadora em potencial. Sem falar nos demais dados heterogêneos que são fornecidos, como análises médicas, passado laboral, a exemplo de muitos extensos questionários a cujo preenchimento se submetem os postulantes a uma vaga no mercado de trabalho. (B) DURANTE A RELAÇÃO EMPREGATÍCIA: as pastas relacionadas aos dados decorrentes da relação empregatícia vai sendo enriquecida com o desenvolver do contrato de trabalho, podendo incorporar dados relativos à duração das interrupções da atividade, resultados de exames médicos, enfermidades, eventuais sanções disciplinares, evolução da formação, carreira profissional, horários de entrada e saída da empresa, movimento no interior desta, modificações na situação familiar, dados bancários, beneficiários de seguro, dados financeiros (salário, etc.). Alguns desses dados são dados pessoais não sensíveis, porém, muitos deles são dados sensíveis que o empregador é obrigado a tomar conhecimento, pois tem obrigação de geri-los, como, por exemplo, quando o empregado se afasta do trabalho por motivo de doença. • (C) APÓS O TÉRMINO DA RELAÇÃO DE EMPREGO: ainda pode o ex-empregador possuir dados relacionados a ações impetradas na Justiça do Trabalho pelos ex-empregados, que podem vir a compor, futuramente, as tão conhecidas 'listas negras' de trabalhadores."

[154] "Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, [...]" (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

[155] "Art. 8º, § 1º: O direito comum será fonte subsidiária do direito do trabalho. (BRASIL. Decreto-Lei nº 5.452, de 1º de maio de 1943).

[156] De acordo com o artigo 5º, inciso IV, o banco de dados consiste no conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico. (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

Por fim, é notória a existência de uma defasagem entre o progresso tecnológico e as soluções jurídicas reguladoras dos problemas que surgem. Diante disso, a lei geral de proteção de dados elenca alguns princípios que devem ser observados nas atividades envolvendo o tratamento de dados, os quais podem servir, inclusive, como parâmetro quando o tratamento de dados ocorrer no curso da relação de trabalho, questão objeto do próximo ponto.

3.3 OS PRINCÍPIOS FUNDAMENTAIS DE TRATAMENTO DE DADOS E SUA APLICAÇÃO NA RELAÇÃO DE TRABALHO

A realidade aponta para a existência de uma desproporção entre os efeitos das novas tecnologias e a mudança de paradigma marcada pelo emergir da informação como recurso fundamental para a organização do futuro. As transformações são imensas a ponto de os ordenamentos jurídicos não acompanharem tal velocidade.[157] As técnicas tradicionais parecem insuficientes. Diante disso, Rototà (2008, p. 57-58) destaca que:

> A verdadeira questão diz respeito à possibilidade de atribuir um valor orientador, para o futuro, a categorias e conceitos que, como o dos contratantes hipossuficientes ou da privacidade, foram elaborados para situações em que a informação como recurso ainda não ocupava a posição central. [...] Estamos, portanto, diante da necessidade de estabelecer qual deve ser o quadro de princípios fundamentais ao qual faremos referência na situação transformada, [...] A era da informação pede também que sejam reescritas as tábuas de valores, justamente para garantir a plena expansão daquilo que sinteticamente indicamos com os termos liberdade e democracia.

Em matéria de proteção de dados, há alguns documentos representativos do que já se encontra consolidado e do que está emergindo. “A atenção deve ser dirigida, por um lado, para os princípios que são afirmados; e, por outro, aos instrumentos necessários para assegurar a sua efetividade.” (RODOTÀ, 2008, p. 59).

---

[157] Quanto ao tema, Bolzan de Morais e Jacob Neto (2018) reforçam que aumentar a produção legislativa, criar emendas constitucionais e resolver possíveis violações nos tribunais não será suficiente para enfrentar algo tão líquido quanto o fluxo de dados e a afetação sobre os direitos fundamentais. Para os autores, a “abordagem fornece uma segurança (jurídica) que, infelizmente, é falsa. Embora sejam uma herança da “modernidade sólida”, os direitos fundamentais são, inquestionavelmente, essenciais para mantermos nossa humanidade em tempos líquidos e, por mais paradoxal que pareça, somente será possível mantê-los por meio de ferramentas caracterizadas pela liquidez, adjetivo tão pouco apreciado pela teoria jurídica.” (BOLZAN DE MORAIS; JACOB NETO, 2018, p. 102).

Assim, como forma de acompanhar a transformação vivenciada, em termos de proteção de dados utilizam-se dois textos de relevância internacional: a Convenção do Conselho da Europa (de 28 de janeiro de 1981, para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal), e a Recomendação da OCDE (de 23 de setembro de 1980, que traça as diretrizes relativas à proteção da privacidade e dos fluxos transfronteiriços de dados pessoais), a partir das quais são deduzidos diversos princípios, como os que seguem:

> 1. *princípio da correção* na coleta e no tratamento das informações;
> 2. *princípio da exatidão* dos dados coletados, acompanhado pela obrigação de sua atualização;
> 3. *princípio da finalidade* da coleta dos dados, que deve poder ser conhecida antes que ocorra a coleta, e que se especifica na relação entre os dados colhidos e a finalidade perseguida (*princípio da pertinência*); na relação entre a finalidade da coleta e a utilização dos dados (*princípio da utilização não-abusiva*); na eliminação, ou na transformação em dados anônimos das informações que não são mais necessárias (*princípio do direito ao esquecimento*);
> 4. *princípio da publicidade* dos bancos de dados que tratam as informações pessoais, sobre os quais deve existir um registro público;
> 5. *princípio do acesso individual*, com a finalidade de conhecer quais são as informações coletadas sobre si próprio, obter a sua cópia, obter a correção daquelas erradas, a integração daquelas incompletas, a eliminação daquelas coletadas ilegitimamente;
> 6. *princípio da segurança* física e lógica da coletânea dos dados. (RODOTÀ, 2008, p. 59).

Muitos desses princípios, já presentes no ambiente europeu, foram incorporados na Diretiva da Comunidade Europeia nº 95/46 de 1995 e na Carta de Direitos Fundamentais da Comunidade Europeia de 2000, servindo, posteriormente, de base para a criação do RGPD, o qual corresponde a uma normativa pautada por princípios e regras no âmbito da União Europeia.[158]

A escolha brasileira, por seu turno, como já referido, aproximou-se do modelo europeu, privilegiando uma legislação por princípios, o que se identifica a partir da redação do artigo 6º da Lei nº 13.709/2018, segundo o qual as atividades de tratamento de dados pessoais, além de observar a boa-fé, devem se pautar pelos princípios da finalidade, da adequação, da necessidade, do livre acesso, da qualidade dos dados, da transparência, da segurança, da prevenção, da não discriminação e da responsabilização e prestação de contas.

---

[158] Remete-se o leitor ao item 3.1 para maior aprofundamento do tema.

Portanto, em matéria de proteção de dados pessoais e sensíveis, as soluções devem passar, como propõe Rodotà (2008, p. 10):

> [...] por uma legislação de princípios e códigos de deontologia – contando estes com a participação direta das categorias profissionais interessadas, que assim melhor podem assegurar a correspondência à realidade do setor – reunida com a finalidade de realizar uma disciplina equilibrada relativamente às mudanças sociais.

Diante disso, antes de adentrar na análise dos princípios e da sua incidência nas relações laborais, convém apresentar algumas definições trazidas pela doutrina acerca do que se entende por *princípio*, uma vez que "desde a promulgação da Constituição de 1988, o debate sobre os princípios jurídicos ganha cada vez mais espaço." (SILVA, 2011, p. 29).

Nessa perspectiva, o jurista Robert Alexy, um das maiores autoridades em matéria de direitos fundamentais, trabalha com a distinção entre princípios e regras, questão essencial para a análise dos efeitos dos direitos fundamentais nas relações entre particulares.

Na visão de Alexy (2008, p. 90), "*princípios* são normas que ordenam que algo seja realizado na maior medida possível dentro das possibilidades jurídicas e fáticas existentes." Ou seja, princípios são *mandamentos de otimização*, que se caracterizam por poderem ser satisfeitos em graus variados, sendo que a medida devida de sua satisfação não depende somente das possibilidades fáticas, mas também das possibilidades jurídicas. Já as regras "são normas que são sempre ou satisfeitas ou não satisfeitas. Se uma regra vale, então, deve se fazer exatamente aquilo que ela exige; nem mais, nem menos." (ALEXY, 2008, p. 91).

Assim, para a resolução de um conflito de regras, Alexy utiliza o raciocínio do tudo-ou-nada, isso porque tal conflito refere-se exclusivamente a um problema de validade. Ao passo que, em caso de colisão de princípios, a solução se dará pelo sopesamento entre os princípios colidentes a fim de se decida qual deles terá preferência no caso concreto.

Portanto, em caso de colisão entre princípios, haverá a possibilidade de limitar, no caso concreto, a realização de um ou mais princípios parcial ou totalmente. E, mesmo neste caso, ao contrário do que ocorre com os conflitos entre regras, nenhum dos princípios será declarado inválido.

Cabe destacar, como alerta Silva (2011, p. 35) que “o termo *princípio* é plurívoco”, sendo importante perceber que há juristas que trabalham com noções diferentes, como é o caso da clássica definição de Celso Antônio Bandeira de Mello, “segundo o qual princípios são ‘mandamentos nucleares’ ou ‘disposições fundamentais’ de um sistema, ou ainda da definição de Canotilho e Vital Moreira, que definem princípios como ‘núcleos de condensações’”. (SILVA, 2011, p. 35-36).

Delineada brevemente a noção de princípio, cabe analisar, à luz do artigo 6º da Lei nº 13.709/2018 e da doutrina especializada, os princípios gerais de proteção que deverão ser observados quando da realização do tratamento de dados pessoais e de que forma eles podem ser aplicados na relação de trabalho, a fim de assegurar uma proteção adequada aos dados dos trabalhadores.

O primeiro relaciona-se ao *princípio da boa-fé.* Trata-se de um princípio geral de Direito que orienta a conduta das partes, tendo como funções interpretar os negócios jurídicos (artigo 113 do Código Civil) e limitar o exercício de um direito (artigo 187 e 422 do Código Civil). Tal princípio, além de ser um dos vetores da relação de trabalho[159], aplica-se aos dados pessoais, na medida em que quem recolhe dados de outrem, trata ou mantém sob sua custódia tem o dever ético de agir com correção, honestidade, confiança e lealdade, não podendo, em seus atos, ultrapassar os limites impostos por este valor. (CHEHAB, 2015). Assim, por força deste princípio:

> [...] a entidade empregadora deve – antes de iniciar o tratamento – informar o trabalhador sobre as condições de utilização dos meios da empresa para fins privados e a realização do seu controlo (formas e metodologias adotadas), sobre a existência do tratamento de dados que lhe está associado, suas finalidades, os dados tratados e o seu tempo de conservação, bem como sobre o grau de tolerância admitido e as consequências da má utilização ou utilização indevida dos meios de comunicação colocados à sua disposição. (CNPD, 2013, p. 11).

O *princípio da finalidade* determina que o tratamento de dados deve ser feito “para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.”

---

[159] Importante notar que “todas as conclusões do direito civil sobre boa-fé nos contratos são aplicáveis ao direito do trabalho. É uma decorrência do princípio da eticidade nos contratos, o que não é reserva do direito civil, mas uma ideia básica comum aos contratos em qualquer setor do direito. O comportamento dos sujeitos dos contratos de trabalho deve respeitar um conjunto de deveres previstos pelo direito positivo, tanto o empregado como o empregador, e boa-fé tanto no período pré-negocial como na constância de contratos e na fase da extinção dos contratos, e o comportamento que contrariar o princípio estará em desacordo com o direito.” (NASCIMENTO, 2011, p. 578).

(BRASIL, Lei nº 13.709, de 14 de agosto de 2018). A propósito, Doneda (2006, p. 216) dispõe que:

> [...] toda utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da sua coleta. Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que é possível a estipulação de um critério para valorar a razoabilidade da utilização de determinados dados para uma certa finalidade (fora da qual haveria abusividade).

No campo laboral, o Repertório de Recomendações da OIT (OIT, 1997) dispõe que os dados pessoais devem ser utilizados apenas para a finalidade para os quais foram coletados e, havendo exploração para outros fins, o empregador deve garantir que eles não sejam usados de forma incompatível com o objetivo inicial e adotar medidas necessárias pra evitar qualquer má interpretação devido a sua aplicação em outro contexto.[160]

O *princípio da adequação* estabelece que deve haver "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento." (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

Com relação ao *princípio da necessidade*, a Lei nº 13.709/2018 dispõe tratar-se de "limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados." (BRASIL, Lei nº 13.709, de 14 de agosto de 2018). Importantes as considerações trazidas por Rodotà (2008, p. 10) acerca deste princípio, na medida em que:

> [...] por constituir uma frontal oposição à tendência humana de utilizar sempre toda e qualquer inovação tecnológica disponível: "o direito não deve render-se à razão tecnológica", complementa o autor. Ainda quanto ao princípio da necessidade, outra regra pôde ser deduzida: é preciso circunscrever a coleta de informações ao mínimo indispensável de modo a garantir a maior liberdade possível. Como compara Rodotà, "nos regimes totalitários, a criminalidade é bem mais controlada; mas o preço é o sacrifício da liberdade de todos". Outra regra, decorrente do mesmo princípio, é a que se refere à estreita correlação entre os dados coletados e as finalidades perseguidas. A

[160] Na visão de Moreira (2016, p. 45-46), o princípio da finalidade "constitui o princípio verdadeiramente cardinal da proteção de dados, sendo os demais princípios função deste na medida em que os dados deve ser adequados, pertinentes e não excessivos em relação à finalidade pretendida; devem ser exatos, completos e atualizados em função da finalidade; e só devem ser conservados pelo tempo que a finalidade exige. Atendendo a este princípio não conseguimos vislumbrar como determinados dados da vida privada do trabalhador, como fotografias onde uma candidata está em *biquíni* ou com uma garrafa de vodka na mão poderão cumprir estes motivos da pertinência, da adequação e da necessidade."

> coleta não pode ser tomada como uma “rede jogada ao mar para pescar qualquer peixe”. Ao contrário, as razões de coleta, principalmente quando se tratarem de “dados sensíveis”, devem ser objetivas e limitadas.

Já o *princípio do livre acesso* garante aos titulares “consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.” Junto deste, há o *princípio da qualidade dos dados* que estabelece a “garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.” E, em igual sentido, há o *princípio da transparência*, que garante, aos titulares, “informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.”[161] (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

No ambiente laboral, o Repertório de Recomendações Práticas da OIT (OIT, 1997) assegura aos trabalhadores o direito a serem informados regularmente sobre os dados pessoais que lhes dizem respeito e sobre seu tratamento, independentemente destes dados estarem sujeitos a processamento automático ou mantidos em um arquivo manual ou em qualquer outro arquivo que inclua seus dados pessoais.

Há, ainda, o *princípio da segurança*, o qual determina que sejam utilizadas “medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.” Reforçando tal diretriz, o *princípio da prevenção* estabelece a “adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.” (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

Refere-se, ainda, o *princípio da não discriminação* que firma a “impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.” (BRASIL, Lei nº 13.709, de 14 de agosto de 2018). Trata-se de um princípio de extrema importância para a seara laboral, uma vez que o tratamento dos dados não deve conduzir a uma discriminação ilícita em matéria de emprego ou ocupação. No tocante, o próprio Repertório (OIT, 1997) reforça este princípio geral de não

---

[161] Um exemplo de aplicação prática do princípio da transparência consiste em levar ao conhecimento do trabalhador ou de seus representantes a existência de um sistema de vigilância e de controle pelo empregador, sendo isso essencial para o tratamento de dados pessoais. Além disso, o controle oculto ou secreto sobre os trabalhadores através de meios audiovisuais viola o princípio da boa-fé empresarial, como destaca Moreira (2016).

discriminação em emprego, substancial para evitar que o uso de dados pessoais e sensíveis comporte, direta ou indiretamente, a discriminação contra pessoas ou grupos de trabalhadores.

Além disso, dada a relevância do tema, a Declaração da OIT sobre os Princípios e Direitos Fundamentais no Trabalho (OIT, 1998) prevê como um de seus princípios *a eliminação da discriminação em matéria de emprego e ocupação*. Menciona-se, também, a existência da Convenção nº 111 e a Recomendação nº 111, ambas da OIT, as quais proíbem tal discriminação, assim como, em âmbito nacional, o artigo 3º, inciso IV, e o artigo 7º, incisos XXX, XXXI e XXXII, ambos da Constituição Federal.

E, por último, o *princípio da responsabilização e da prestação de contas*, o qual consiste na "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas." (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

Assim, tal arcabouço principiológico, além de orientar as atividades que envolvem o tratamento de dados pessoais, servem como guia para o processamento na área trabalhista, observadas as particularidades que tal relação envolve.

Nesse sentido, haverá casos em que mesmo dados pessoais sensíveis deverão ser de conhecimento do empregador. Em tais situações, havendo dúvidas quanto à existência de legítimo interesse por parte de quem os trata, o balanceamento de direitos, amparado em princípios, permitirá verificar se as legítimas expectativas e os direitos e liberdades fundamentais do trabalhador estão sendo respeitadas.[162]

Não obstante, vale mencionar que o Repertório de Recomendações Práticas da OIT ilustra alguns casos em que, apesar da sensibilidade de alguns dados, nem sempre é possível descartar pura e simplesmente a sua coleta. Nesse ponto, o Repertório (OIT, 1997) exemplifica a situação envolvendo a contratação de um jornalista para trabalhar em jornal afiliado a um determinado partido político, caso em que é preciso levar em consideração as ideias políticas do profissional. Na hipótese, o fato de os dados serem sensíveis não é suficiente para excluí-los da tarefa de coleta, porém é preciso respeitar certos princípios, a fim de compensar a posição mais vulnerável dos trabalhadores.

---

[162] Para maior aprofundamento, remete-se o leitor ao item 4.1.

Dessa forma, o Repertório apresenta uma série de situações nas quais o recolhimento de dados só deve ser autorizado em caráter excepcional e apenas quando tenham relação direta com uma decisão em matéria de emprego. Trata-se de hipóteses em que a coleta deve ser feita em conformidade com a legislação nacional, com as leis contra a discriminação ou com os regulamentos sobre o tratamento de dados sensíveis, compreendidos nas leis nacionais.

Feitas tais considerações, analisa-se as hipóteses previstas no Repertório. A primeira delas diz respeito aos dados referentes à vida sexual dos trabalhadores.[163] Segundo o Repertório, estes dados podem ser obtidos quando houver uma acusação de assédio sexual, devendo ser utilizados apenas para este fim.

Quanto aos antecedentes criminais, por se tratar de um dado potencializador de discriminação do empregado, a coleta deve limitar-se a alguns circunstâncias, como, por exemplo, quando envolve cuidado de filhos, pois o candidato pode ter sido condenado por molestar uma criança, ou, no caso de motorista profissional, este deve divulgar as penalidades criminais a que submetido por dirigir em estado de embriaguez.[164] Segundo o Repertório da OIT, este tipo de dado deve ser obtido diretamente do interessado, para ter certeza de que a coleta não vá além do necessário.

---

[163] No que tange ao aspecto sexual, é preciso lembrar que a orientação sexual configura um dado pessoal sensível do trabalhador, o qual, se objeto de questionamento ou de revelação, pode conduzir a situações de assédio e de discriminação no ambiente de trabalho. Além disso, vale lembrar que o novel artigo 223-C da CLT inclui a sexualidade como um dos bens jurídicos tuteláveis, inerente à pessoa física. (BRASIL. Decreto-Lei nº 5.452, de 1º de maio de 1943).

[164] Apostolides (2008) deixa claro que o empregador só pode colocar questões sobre o tema dos antecedentes penais se a informação que visa recolher for relevante para a prestação da atividade laboral. Nesse sentido, elenca algumas situações, tais como, quando houver risco de repetição da atividade criminosa (ex.: é possível perguntar ao caixa de um banco se já foi condenado pela prática do crime de furto), quando a atividade apresentar em si um risco acrescido de lesão de bens penalmente tutelados (ex.: caso do vendedor de uma loja de espingardas ou do vigilante de segurança privada), pois sobre o empregador recai um dever de garantir a segurança do local de trabalho, podendo vir a ser responsabilizado por terceiros pelos atos praticados pelo trabalhador, ou, o interesse legítimo do empregador se justifica quando esteja em causa uma relação de confiança. Quanto a esta hipótese, Apostolides (2008, p. 252) pondera que "não se trata de legitimar o afastamento de um candidato com base em valorações subjectivas do empregador assentes em orientações sociais e éticas, mas sim assentes na própria natureza da actividade, que pressupõe uma relação de confiança. Seria o caso do director administrativo, da secretária pessoal ou da empregada doméstica." Por fim, a autora (2008) menciona o caso em que esteja em causa uma organização de tendência, cuja orientação ideológica seja avessa à prática de crimes (ex.: organização ambientalista que tem, naturalmente, todo o interesse em averiguar a prática de crimes contra o ambiente). Cabe salientar que em tais situações as perguntas sobre os antecedentes penais são legítimas, devendo o trabalhador responder com verdade, sob pena de o contrato ser anulado por erro ou dolo e incorrer em responsabilização pré-contratual. Porém, a doutrina também entende que, se decorrido um justo prazo, a ponto de até mesmo o registro do crime ter sido cancelado, não subsistiria o dever de informar, e desde que não tenha ocorrido nova condenação por crime. (APOSTOLIDES, 2008).

Em relação à filiação sindical,[165] as empresas podem coletar dados apenas para cumprir as disposições relativas à dedução da contribuição sindical ou para facilitar o funcionamento das comissões de empresa, por exemplo. A legalidade desta coleta decorre da própria norma trabalhista, na medida que cabe aos empregadores informarem aos representantes dos trabalhadores tais questões. Da mesma forma, os representantes devem manter todo o tipo de precaução para impedir que as informações caíam nas mãos de terceiros não autorizados a conhecê-las.

E quanto à coleta de dados[166] médicos [167], deve se restringir ao necessário para determinar se o trabalhador é apto para um trabalho específico, para cumprir as regras de segurança e saúde no trabalho e para ter direito a benefícios sociais, sob pena de haver uma utilização prejudicial da informação, a ponto de a empresa criar uma situação de desigualdade, como no exemplo trazido por Limberger (2009, p. 43-44):

> No que se refere à saúde, um portador do vírus HIV pode não ser contratado em virtude da doença ou ser despedido. A possibilidade de a empresa escolher um trabalhador sadio, no momento da contratação, é muito grande, o que caracterizaria uma discriminação.

Por isso, salvo em um número restrito de atividades profissionais pode ser pedido o exame HIV, ou seja, aqueles em que o empregado realiza uma atividade

---

[165] No entender de Apostolides (2008, p. 248), é possível fixar que "a regra nesta matéria é a de que as perguntas sobre filiação sindical do candidato não devem ser admitidas, por não apresentarem qualquer relevância para a prestação da actividade profissional ou para a avaliação da capacidade ou aptidão do trabalhador." Assim, formulações sobre filiação sindical "não são legítimas numa fase *prévia* à celebração do contrato, pelo simples facto de que eles não dizem respeito ao trabalhador nem à prestação da actividade laboral, mas sim ao exercício de obrigações que o empregador deve assumir no decurso da relação contratual."

[166] Acerca dos dados relativos à saúde, "em se tratando de categorias e atividades específicas, nas quais uma sanidade é fundamental, sob pena de colocar em risco o próprio trabalhador e os demais, há de se entender pela possibilidade de serem os dados, mesmo que sensíveis, recolhidos e tratados, independentemente de autorização do trabalhador. É o caso, por exemplo, dos trabalhadores das áreas de transportes e segurança, aos quais se impõe o efetivo controle sobre o consumo de drogas e álcool, em nome da potencialidade danosa do exercício dessas atividades sob seus efeitos." (STIVAL, 2015, p. 138). Em complemento, menciona-se, no Brasil, a existência da Lei nº Lei nº 13.103, de 02 de março de 2015. Trata-se de lei específica que autoriza a realização do exame toxicológico para os motoristas profissionais de transporte rodoviário de passageiros e de cargas (artigo 1º, parágrafo único, incisos I e II, da Lei nº 13.103/2015).

[167] Ainda sobre o tema, para maior aprofundamento, recomenda-se a leitura da obra de Apostolides (2008), na qual a autora aborda diversas situações em que perguntas sobre a saúde e estado de gravidez da trabalhadora são legítimas. De forma resumida, os questionamentos serão legítimos "quando esteja em causa a impossibilidade de prestar ou quando tal seja justificado por razões de segurança e saúde do trabalhador e de terceiros, independentemente dessas razões resultarem da natureza da actividade a prestar ou da componente organizacional do contrato de trabalho." (APOSTOLIDES, 2008, p. 244).

que, se for portador da enfermidade, pode causar um contágio. Há de se ponderar a proteção individual do trabalhador com o perigo de expor a saúde da coletividade.

Com relação ao tema, para evitar que os dados pessoais do trabalhador, em especial, os dados sensíveis sejam utilizados para fins discriminatórios, o Repertório de Recomendações da OIT propõe nas cláusulas 10.8 e 10.9 que o empregador não tenha acesso direto aos resultados dos exames, mas tão somente à indicação da aptidão ou não do trabalhador para realizar a atividade proposta, ou ainda, a indicação dos tipos de trabalhos que, temporária ou definitivamente, lhe estão contraindicadas.

Atenta-se, também, para o fato de que as informações inerentes a cada trabalhador são manipuladas pelo empregador ou por prepostos, havendo a necessidade da instituição de marcos regulatórios específicos e adequados, bem como de políticas e procedimentos que garantam a segurança dos dados, por meio da implementação de mecanismos de mitigação dos riscos adotados, sob pena de responsabilização das empresas.[168]

Assim, além da criação de mecanismos para salvaguardar os dados pessoais no ambiente de trabalho, especialmente na perspectiva preventiva, é preciso enfrentar a proteção aos dados como um novo direito fundamental do trabalhador, o qual deve ter conhecimento e controle sobre seus próprios dados, visto que representam expressão direta de sua própria personalidade, questão esta a ser abordada no tópico seguinte.

3.4 A PROTEÇÃO DOS DADOS PESSOAIS E SENSÍVEIS COMO DIREITO FUNDAMENTAL DO TRABALHADOR

Com a expansão da realidade digital, os direitos fundamentais, especialmente a privacidade, a intimidade e os dados pessoais e sensíveis do trabalhador, encontram-se ainda mais expostos.[169] Em decorrência disso, a própria

---

[168] Quanto à responsabilidade no tratamento de dados e às políticas e procedimentos a serem adotados no ambiente laboral, remete-se o leitor aos itens 4.3 e 4.4 para maior aprofundamento.

[169] A doutrina diverge quanto ao uso das expressões ‘privacidade’ e ‘intimidade’. Doneda (2006) considera que a utilização do termo privacidade corresponde à opção mais correta, pois é tomada, frequentemente, pela doutrina especializada como gênero do qual são espécies a intimidade e a vida privada, razão pela qual ele prefere utilizar o vocábulo ‘privacidade’. Partindo disso, Ruaro e Rodriguez (2010, p. 165-166) consideram que “a intimidade pode ser definida como o modo de ser de determinado indivíduo, consistindo fundamentalmente na exclusão do conhecimento pelos demais daquilo que

noção de privacidade passou por uma releitura: o notório conceito do “direito a ficar só” ou “direito a ser deixado em paz" já não atende aos atuais anseios sociais, estando superado, nascendo, assim, a privacidade como “direito à autodeterminação informativa”, que concebe a cada pessoa um real poder de controle sobre suas próprias informações, seus próprios dados.

O *right to be let alone* ou “direito a ficar só”, enunciado pelo juiz norte-americano Cooley, foi um dos alicerces do célebre artigo de Brandeis e Warren, *The right to* privacy, pioneiro ao estabelecer um marco na doutrina do direito à privacidade, além de antever a importância que a matéria assumiria com o desenvolvimento das tecnologias de informação, pois já naquela época o artigo enfocava a tecnologia como provedora dos meios que possibilitavam a intromissão indevida em assuntos privados: a fotografia, a imprensa, as gravações, todas em contínuo desenvolvimento. (DONEDA, 2000).

Ao traçar uma breve evolução quanto à noção de privacidade, Doneda (2000) aponta que a Bíblia, os textos gregos clássicos e, até mesmo os da China antiga, faziam menção à privacidade, enfocando-a como o direito ou a necessidade da solidão.

---

somente a ele diz respeito. Corresponde, então, a todos os fatos, informações, acontecimentos ou eventos que a pessoa deseje manter em seu foro íntimo.” Doneda (2006) indica que a expressão “intimidade” relaciona-se com o direito à vida tranquila, ou também, com o *right to bel et alone*. Acrescenta que a distinção entre o direito à vida privada e o direito à intimidade já foi compreendida pela teoria alemã dos círculos concêntricos, a qual encontra-se superada, sendo referida pela doutrina alemã como ‘teoria da pessoa como uma cebola passiva’. (Doneda, 2006, p. 108). A referida teoria determinava que o maior dos círculos abrangeria os demais, até chegar ao círculo nuclear, sendo que cada uma das esferas representaria os diferentes graus de manifestação da privacidade: a esfera da vida privada (*privatshäre*) corresponderia a mais ampla de todas, abrangendo todo o material, fato ou circunstância que o indivíduo pretende deixar longe do alcance dos demais, podendo ser conhecido apenas por aqueles que têm contato regular com a pessoa; a esfera confidencial (*vertrauensphäre*) equivaleria àquela que não deve ser conhecida nem mesmo pelos que entram em contato com a vida privada; e a esfera do secreto ou da intimidade (*geheimsphäre*) corresponderia aos assuntos que jamais deveriam ser conhecidos pelos outros, dada a sua natureza fundamentalmente íntima. No Brasil, esta teoria foi acrescida por um quarto círculo, na seguinte ordem de abrangência: público – privacidade – intimidade – segrego. Importante mencionar que a superação da teoria dos círculos concêntricos no direito alemão ocorreu em 1983, a partir da Sentença do Censo (*volkszählungsurteil*) pelo tribunal Constitucional, a qual resolveu uma questão de inconstitucionalidade que havia na Lei, ao prever uma ampla revelação dos dados pessoais da população. Foram definidos traços primordiais do direito à proteção de dados pessoais, denominado ‘direito à autodeterminação informativa’ (*das informationelle selbsbestimmungsrecht*), segundo a qual o sujeito devia decidir quando e sob que circunstâncias quer dar conhecimento dos seus dados. Segundo Bioni (2019, p. 104), o julgado é paradigmático “ao não tomar a proteção de dado pessoais como uma evolução do direito à privacidade. Pelo contrário, tratá-lo como um direito de personalidade autônomo que reclama uma técnica de proteção desconectada da dicotomia entre público e privado.”

Na Inglaterra do século XVII, estabeleceu-se o princípio da inviolabilidade do domicílio – *man´s house is his castle*[170]*,* que originaria a tutela de alguns aspectos da vida privada relacionados com o respeito ao *domus*, ao espaço físico privado do homem. Na época feudal, a casa da família passou a representar um espaço de intimidade, com a separação da vida da comuna. Com o surgimento do homem burguês, junto com sua necessidade da propriedade privada, aparece também a de uma vida privada. O burguês passou a se isolar dentro de sua própria classe, de sua própria casa, de sua propriedade. A privacidade, como garantia de isolamento e solidão, representava a exigência de uma classe, quase que um privilégio alcançado por alguns.

Foi em 1890, ano em que publicado o artigo *The right to privacy* e também concebida a máquina eletromecânica do norte-americano Herman Hollerith[171], capaz de realizar o censo de seu país em um terço do tempo do censo anterior, que houve um dos primeiros passos de uma tecnologia que proporcionaria uma redefinição dos limites do direito à privacidade.

Na sequência, em 1946, a fim de facilitar cálculos numéricos, foi ligado o ENIAC (*Eletronic Numerical Integrator Analyzer and Computer* ou computador integrador numérico eletrônico), primeiro computador eletrônico, cuja capacidade de processar e armazenar informações multiplicou-se, o que permitiu a manipulação de dados em grande escala para a época.

Somado a isso, a segunda guerra mundial e a guerra fria impulsionaram a evolução dos computadores e sua capacidade de processar informações ao demandar novos sistemas de telecomunicações. Desse modo, foi possível recolher um maior número de dados, processá-los rapidamente e combiná-los para as mais diversas finalidades, tudo num curto espaço de tempo, dando origem aos bancos de dados.

> O hábito de coletar informações sobre cidadãos há muito era conhecido do Estado. Antes dele, a Igreja organizou durante séculos registros sobre as populações de determinados locais, tarefa que passou a ser realizada pelo Estado quando os meios tornaram-na possível e a questão passou a ser determinante para definir estratégias de desenvolvimento. O cidadão pôde se beneficiar disso ao obter certidões e documentos da administração pública com maior presteza, assim como os governos puderam ter uma noção mais

---

[170] A casa do homem é o seu castelo (tradução nossa).
[171] Doneda (2000) refere a máquina de Hollerith como o primeiro processamento mecânico de informações.

> exata das necessidades da população. [...] Logo o processamento de informações se colocou também ao alcance de entes privados. Os meios financeiro e comercial foram os primeiros a se beneficiarem das novas possibilidades. Ao passarem a utilizar bancos de dados com informações sobre a situação econômica de clientes, criaram uma proteção contra maus pagadores e incentivando os mais fiéis. (DONEDA, 2000, p. 05).

Com as transformações advindas dos acontecimentos relatados, houve a evolução do conceito de privacidade, como “o direito a ser deixado em paz” para a perspectiva de “controle sobre as próprias informações”. O sentido de isolamento inicialmente existente já não atendia aos novos desafios, a noção de privacidade passava a exigir uma concepção mais ampla:

> [...] no direito ao respeito à vida privada e familiar manifesta-se, sobretudo, o momento individualista e o poder exaure-se substancialmente na exclusão da interferência de outrem; a tutela, portanto, é estática e negativa. Já a proteção dos dados pessoais, ao contrário, fixa regras sobre a modalidade de tratamento dos dados e concretiza-se em poderes de intervenção; a tutela é dinâmica, segue os dados em sua circulação. (RODOTÀ, 2008, p. 08).

Nesse sentido, a ampliação do conceito de privacidade decorre:

> [...] em grande medida, por conta da evolução das formas de divulgação e apreensão de dados pessoais. Com o advento de novas tecnologias, notadamente o desenvolvimento da biotecnologia e da Internet, o acesso a dados sensíveis e, consequentemente, a sua divulgação, foram facilitados de forma extrema. Como resultado, existe uma expansão das formas potenciais de violação da esfera privada, na medida em que se mostra a facilidade por meio da qual é possível o acesso não autorizado de terceiros a esses dados. Com isso, a tutela da privacidade passa a ser vista não só como o direito de não ser molestado, mas também como o direito de ter controle sobre os dados pessoais e, com isso, impedir a sua circulação indesejada. (BODIN DE MORAES, 2018, p. 42).

Tomando como base essa nova perspectiva, Bodin de Moraes (2018, p. 52-57) ainda elenca a existência de três diferentes concepções sobre o direito à privacidade:

> (i) O direito a ser deixado só, em acepção originária, tradicional, e referenciada a um período de liberalismo político e econômico, que direcionava a proteção da privacidade a um ideal burguês de tutela patrimonial; (ii) O direito de ter controle sobre a circulação dos dados pessoais, determinado por meio da construção teórica e jurisprudencial da denominada autodeterminação informativa, estabelecendo a prerrogativa da pessoa de acessar, corrigir, controlar e disponibilizar dados pessoais, somente por sua livre escolha; e (iii) O direito à liberdade das escolhas pessoais de caráter existencial, representando a ligação entre a autonomia existencial da pessoa e a construção de sua identidade pessoal por meio da

> proteção de seus dados sensíveis – i.e. posição política, expressão partidária, afiliação sindical, opção sexual, condições de saúde, etc (dignidade).

Além disso, tal evolução confere uma supervisão e poderes não somente às pessoas interessadas (os sujeitos dos dados), mas também a uma autoridade independente.[172] "A proteção não é mais deixada somente aos sujeitos dos dados, uma vez que existe um órgão público permanente responsável por isso. Logo, há uma redistribuição de poderes sociais e legais se formando." (RODOTÀ, 2008, p. 17). Acerca da possibilidade de controle exercido pelo cidadão sobre as organizações públicas e privadas que recebem as informações, resultando em um crescente *plus-poder* destas, Rodotà (2008, p. 37) faz o seguinte alerta:

> [...] seria evidentemente irrealizável se a perspectiva do controle permanecesse somente individual, resolvendo-se completamente na atribuição a cidadãos isolados do direito de acesso aos bancos de dados públicos e privados.
> Raramente o cidadão é capaz de perceber o sentido que a coleta de determinadas informações pode assumir em organizações complexas e dotadas de meios sofisticados para o tratamento de dados, podendo escapar a ele próprio o grau de periculosidade do uso destes dados por parte de tais organizações. Além disso, é evidente a enorme defasagem de poder existente entre o indivíduo isolado e as grandes organizações de coleta de dados: nessas condições, é inteiramente ilusório falar em "controle". Aliás, a insistência em meios de controle exclusivamente individuais pode ser o álibi de um poder público desejoso de esquivar-se dos novos problemas determinados pelas grandes coletas de informações, e, que assim se refugia em uma exaltação ilusória dos poderes do indivíduo, o qual se encontrará, desta forma, encarregado da gestão de um jogo do qual somente poderá sair como perdedor.
> A atenção, consequentemente, deve deslocar-se dos meios de reação individual para instrumentos de controle social: e poderá ocorrer que, seguindo esse caminho, alguns meios que estavam tradicionalmente à disposição do indivíduo venham a ser perdidos; perda, no entanto, que pode

---

[172] A Convenção Europeia dos Direitos do Homem, em seu artigo 8º, ao dispor sobre o direito ao respeito pela vida privada e familiar, previu a figura da autoridade pública ao definir critérios para o processamento de dados, estabelecendo que a conformidade das regras deve ser submetida ao controle de uma autoridade independente. (CONSELHO DA EUROPA, 1950). No Brasil, a figura da Autoridade Nacional de Proteção de Dados (ANPD), prevista no PLC nº 53/2018, foi vetada no texto final da LGPD, sancionado pelo Presidente Temer, sob o argumento de que o Poder Legislativo não poderia criar órgãos que resultassem em novos gastos ao orçamento do Executivo. Posteriormente, a Lei nº 13.853, de 08 de julho de 2019, criou a ANPD (considerada autoridade nacional), como órgão da administração pública federal, vinculada à Presidência da República, responsável por zelar, implementar e fiscalizar o cumprimento da LGPD no Brasil, assim como elaborar a Política Nacional de Proteção de Dados e da Privacidade, entre outras competências previstas no artigo 55-J da Lei nº 13.709/2018. (CAVALCANTI; SANTOS, 2018. p. 362). Com relação à Autoridade Nacional, Schreiber (2018) crítica o fato de estar vinculada ao poder público, na medida em que a "experiência de outros países mostra, ainda, que a autonomia e independência da Autoridade Fiscalizadora afigura-se indispensável, pois o Poder Público, não raro, é um dos grandes violadores da privacidade dos cidadãos. Daí o equívoco, a meu ver, de propostas que já começam a ser discutidas no Brasil para atribuir tal poder de fiscalização a órgãos de segurança que integram o Poder Executivo Federal."

> ser compensada pela criação, em nível coletivo, de um aparato de controle globalmente mais incisivo e vigilante do que o atual.

Por outro lado, os usuários podem limitar o fluxo de dados que liberam ou compartilham no âmbito das múltiplas relações sociais das quais participam. Contudo, tal medida, por si só, não é suficiente para protegê-los de eventuais danos aos seus direitos fundamentais de personalidade.

Em um mundo digitalizado, a expansão do volume de conteúdo multimídia, juntamente com *smartphones* e mídias sociais, desempenham expressivo papel na coleta de dados pessoais. Logo, é preciso entender como estes afetam a vida dos usuários. A dignidade das pessoas está em risco. Daí a importância de a proteção aos dados pessoais e sensíveis serem compreendidos como um novo direito fundamental tutelado pelo Estado:

> É óbvio que os dados pessoais têm muito a ver com a intimidade ou a privacidade das pessoas, e que sua proteção pode ser abordada em grande parte através dos direitos que protegem a esfera pessoal e privada, consagrados há muito tempo, com uma ou outra formulação, na maior parte das declarações e cartas de direitos humanos ou direitos fundamentais. Mas não há correspondência absoluta entre os dados pessoais e a área pertencente à intimidade ou à vida privada das pessoas. Nem todos os dados pessoais são dados íntimos, nem a privacidade é limitada aos dados pessoais, como é bem sabido. Existem dados pessoais que são públicos, notórios ou acessíveis por natureza ao conhecimento de outras pessoas, como a imagem corporal. Existem espaços da vida privada e familiar que não constituem dados pessoais em sentido próprio, nem podem ser traduzidos em dados pessoais, como é o caso do recinto doméstico, que não coincidem exatamente com a noção de domicílio. E há dados pessoais que, para certos fins, são dados privados, mas também dados públicos ou suscetíveis de conhecimento por outras pessoas, como acontece com os dados de identificação oficial.
>
> Portanto, os direitos à intimidade ou à vida pessoal e familiar, que são os mais próximos desse campo pessoal, se tomarmos como referência as listas mais clássicas desse tipo de direitos básicos, não podem fornecer cobertura completa, ou completamente adequada, em relação aos dados pessoais. São necessários, para este fim, outros instrumentos mais especializados ou sofisticados. É necessário, para ser mais direto, a criação ou identificação de novos direitos, que obviamente podem operar como ingredientes específicos dentro desses outros direitos mais clássicos, mas que também podem aparecer ao seu lado, como direitos com autonomia e substantividade próprias, mesmo que não dispensem completamente suas conexões genuínas com o correspondente direito matriz. É o caso do direito à proteção de dados pessoais, que já começa a se distinguir como tal e a ocupar seu lugar nas mais modernas declarações e cartas de direitos, não obstante o fato de que normalmente o faz sem estar longe dos direitos que em última análise lhe deram impulso (intimidade ou vida privada). Como nosso Tribunal Constitucional já disse, trata-se de um direito que tem por objeto específico

> garantir às pessoas um poder de controle sobre o uso e o destino de seus dados pessoais.[173] (MURCIA; CARDO, 2019, p. 02, tradução nossa).

Compartilhando desse entendimento, Bioni (2019, p. 92) também defende a proteção dos dados como uma categoria autônoma dos direitos da personalidade:

> [...] o direito à proteção dos dados pessoais reclama uma normatização própria que não pode ser reduzida a uma mera "evolução" do direito à privacidade, mas encarada como um novo direito da personalidade que percorre, dentre outras liberdades e garantias fundamentais, a liberdade de expressão, de acesso à informação e de não discriminação. Em última análise, trata-se da nossa própria capacidade de autodeterminação.

Reconhecer que as pessoas vivem em um mundo globalizado e interconectado, no qual os dados circulam pelo mundo virtual sem se submeterem aos tradicionais controles e limites democrático-territoriais é o primeiro passo. A partir daí, necessário se faz repensar o papel do Estado-nação no controle dos fluxos globais de dados, pois, como alerta Ruaro e Rodriguez (2010, p. 165) "a solução para este problema global não poderá ser encontrada isoladamente, senão em conjunto com todas as culturas e sociedades", caso contrário haverá uma vulneração ainda maior na proteção aos direitos fundamentais, isso porque:

---

[173] *Es obvio que los datos personales tienen mucho que ver con la intimidad o privacy de las personas, y que su protección puede abordarse en buena medida a través de los derechos que protegen la esfera personal y privada, consagrados desde hace tiempo, con una u otra formulación, en la mayor parte de las declaraciones y cartas de derechos humanos o derechos fundamentales. Pero no hay coincidencia absoluta entre los datos personales y zona perteneciente a la intimidad o la vida privada de las personas. Ni todos los datos personales son datos íntimos, ni la privacidad se limita a los datos personales, como es bien sabido. Hay datos personales que son públicos, notórios o accesibles por naturaleza al conocimiento de otras personas, como la imagen corporal. Hay espacios de la vida privada y familiar que no constituyen datos personales en sentido propio, ni se pueden traducir sin más en datos personales, como es el caso del recinto doméstico, que no coincide exactamente con la noción de domicilio. Y hay datos personales que a determinados efectos son datos privados pero que también son datos públicos o susceptibles de conocimiento por otras personas, como ocurre con los datos de identificación oficial.*
Por ello, los derechos a la intimidad o a la vida personal y familiar, que son desde luego los más próximos a este terreno personal si tomamos como referencia las listas más clásicas de esa clase de derechos básicos, no pueden prestar cobertura completa, o completamente adecuada, respecto de los datos personales. Son necesarios, con ese fin, otros instrumentos más especializados o sofisticados. Se requiere, por decirlo de modo más directo, la creación o identificación de nuevos derechos, que desde luego pueden operar como ingredientes particulares en el seno de aquellos otros derechos más clásicos, pero que también pueden aparecer a su lado, como derechos com autonomía y sustantividad propias, aunque no lleguen a prescindir por completo de sus genuínas conexiones con el correspondiente derecho matriz. Es el caso del derecho a la protección de datos personales, que ya empieza a distinguirse como tal y a ocupar un lugar propio en las más modernas declaraciones y cartas de derechos, sin perjuicio de que normalmente lo haga a no mucha distancia de los derechos que a fin de cuentas le han dado impulso (intimidad o vida privada). Como ya dijera nuestro Tribunal Constitucional, se trata de un derecho que tiene por objeto específico garantizar a las personas un poder de control sobre el uso y destino de sus datos personales.

> [...] os modelos de direito e de Estado vigentes demonstram pouca – ou nenhuma – capacidade para lidar com conflitos que envolvem as novas tecnologias, intrinsicamente desespacializadas. Não se trata, aqui, de propor o fim do Estado, mas, pelo contrário, de reconhecer que a coleta e o processamento de dados pessoais são questões de relevância pública que escapam, em grande parte, ao controle estatal. Em vez da clássica *quis custodiet ipsos custodes?*, deve-se perguntar qual a legitimidade democrática das categorias em que os indivíduos são classificados. Somente mediante a democratização e a transparência desses critérios será possível proteger os direitos fundamentais, ou seja, tornar-se-á as relações de (in)visibilidade mais visíveis. (BOLZAN DE MORAIS; JACOB NETO, 2018, p. 88).

Partilhando de semelhante sentimento, Bodin de Moraes (2018, p. 77) aduz que:

> [...] dói reconhecer o descompasso entre a rapidez do progresso tecnológico e a lentidão da capacidade de elaboração de instrumentos jurídicos que moldurem essa nova realidade. Com base nesta constatação, é preciso pensar remédios institucionais mais adequados (políticas regulatórias, por exemplo), na medida em que os remédios jurídicos existentes (normas jurídicas proibitivas) encontram-se engessados, obsoletos ou fadados à obsolescência, na medida em que a tecnologia vai se aprimorando e evoluindo.

Para enfrentar o fenômeno informático que atua com extrema velocidade, desafiando o ritmo mais lento com o qual atuam os operadores do direito, Limberger (2009) propõe uma reaproximação da normatividade dos princípios. Segundo a autora (2009, p. 34), “de longo tempo os princípios estão no direito, a novidade é sua estatuição constitucional.” Apoiando-se nisso, propugna:

> [...] uma construção ou uma leitura dos direitos fundamentais com base nos valores superiores do ordenamento jurídico: a liberdade, a justiça, a igualdade e o pluralismo político, bem como na dignidade da pessoa, na perspectiva do fenômeno informático. A informática atuando a serviço do homem, e não como restritiva dos direitos fundamentais. (LIMBERGER, 2009, p. 34).

Assim, a necessidade de proteção aos dados pessoais e sensíveis provocou o surgimento de um novo eixo no que tange à tutela da privacidade, uma vez que o seu titular deseja manter um controle exclusivo sobre o conjunto de ações privadas que lhe dizem respeito (comportamentos, preferências e opiniões). Tal tutela há de basear-se em um novo "direito à autodeterminação informativa", atualmente

presente em diversos ordenamentos[174], que estabelece condições para um efetivo controle das informações pessoais em circulação.[175] (DONEDA, 2000).

> Essa mudança de enfoque, que culminou na concretização da proteção de dados pessoais como direito fundamental da pessoa humana, é resultado das mudanças sociais ocorridas durante os séculos XX e XXI. Com o fortalecimento e ampliação da sociedade industrial e, consequentemente, da de consumo, que se deu, especialmente, a partir de meados do século XX, os dados pessoais passaram a ter importância ímpar e valor econômico, em razão, principalmente, do surgimento das relações massificadas, seja de consumo ou de trabalho. Surgiram, a partir de então, empresas especializadas em recolhimento e tratamento de dados pessoais para posterior venda a interessados, o que veio a causar inúmeros prejuízos às pessoas diretamente envolvidas e também à coletividade. A decisão do Tribunal Constitucional Alemão, datada de 1983, foi, de certa forma, uma imposição de limites a tais práticas invasivas e danosas a direito fundamental. (STIVAL, 2015, p. 131).

No sistema europeu vige o entendimento de que o direito à proteção de dados pessoais é direito fundamental autônomo, digno, por si só, de todos os atributos e prerrogativas concernentes aos direitos fundamentais.[176] Todavia:

> Entre nós, a proteção dos dados pessoais ainda não constitui categoria de direito independente e autônomo do direito à privacidade ou ao segredo das comunicações. Esse fato demonstra certo atraso legislativo na maneira de conduzir a proteção à pessoa. Diversos ordenamentos jurídicos, não só do continente europeu (França, Espanha), mas também da América Latina (México), abordam a questão como de direito fundamental. (WEINSCHENKER, 2013, p. 15).

Porém, no Brasil, como mencionado, em 2018 houve a aprovação da lei geral em matéria de proteção de dados.

---

[174] Menciona-se as Constituições de Portugal e Espanha.

[175] Murcia e Cardo (2019) destacam que, embora o surgimento de um novo direito possa levar ao surgimento de novas frentes regulatórias, estas não precisam ser exclusivamente protetivas. Segundo os autores, regular o "tráfego" de dados pessoais por meio de canais capazes de garantir, ao mesmo tempo, a proteção adequada das pessoas afetadas e o legítimo exercício das atividades de nossa vida é fundamental, pois sem acesso a dados pessoais seria muito difícil o desenvolvimento não apenas das relações econômicas e comerciais, mas também de outras facetas da realidade social, muitas delas ligadas a direitos básicos ou fundamentais para o nosso modo de vida.

[176] A respeito do tema, Weinschenker (2013, p. 15) pondera que “do contato com o sistema normativo da União Europeia, percebe-se que a proteção à privacidade no contexto das novas tecnologias tem sido feita em uma escala maior, através da proteção dos próprios dados pessoais, diretamente. Tal dado parece demonstrar que a proteção legislativa adequada para a problemática residiria, em hipótese, nesse ‘plano elevado’ de proteção: a partir dos dados pessoais, que englobam, sucessiva e obrigatoriamente, a privacidade, e não somente pelo viés da privacidade protegida pela tutela jurídica da personalidade, tal como feito em nosso país.”

Ainda, a propósito do tema, recentemente o Plenário do Senado Federal aprovou a Proposta de Emenda à Constituição (PEC) nº 17, de 2019, que inclui expressamente no texto constitucional o direito à proteção de dados pessoais. Contudo, tal previsão desencadeou controvérsia entre estudiosos da área, isso porque há quem sustente ser desnecessária tal inclusão no texto constitucional, sendo este o entendimento do jurista Anderson Schreiber.

Para Schreiber (2019), a previsão expressa no rol de direitos fundamentais possui um valor simbólico de valorizar o esforço do legislador na edição da LGPD. Porém, emendas constitucionais "não deviam ser propostas com propósitos puramente simbólicos. Bem vistas as coisas, a PEC 17/2019 é inteiramente desnecessária e, mais que isso, perigosa."

De forma resumida, o jurista (2019) argumenta que a proteção de dados pessoais já vem sendo extraída pela doutrina de outras normas constitucionais explícitas, como a proteção à privacidade (art. 5º, X) e a própria cláusula geral de proteção da dignidade da pessoa humana (art. 1º, III), entre outros dispositivos.[177] Além disso, defende ser perigosa tal inclusão, pois "é mexer inutilmente naquilo que deveria ser preservado." (SCHREIBER, 2019).

Ainda, outro ponto crítico da PEC 17/2019 é quanto à questão da competência para legislar sobre proteção de dados pessoais, pois prevê que esta é privativa da União. No entender de Schreiber (2019), ao invés de ampliar a proteção aos dados, isso traz severo risco de limitá-la, fulminando iniciativas que já se encontram em vigor em defesa da privacidade.

Por outro lado, os que defendem a inclusão expressa da proteção dos dados como um direito fundamental argumentam que a sua previsão na Constituição Federal tornará o Estado um garantidor desse direito, pois passará a ter um compromisso maior com a tutela dos dados pessoais de seus cidadãos. Tal posição é defendida pela Relatora da PEC, a Senadora Simone Tebet (MDB-MS), a qual assevera que "constitucionalizar a questão significa o Estado dizer que reconhece a importância do tema, classificando esse direito à proteção de dados como fundamental". (SENADO NOTÍCIAS, 2019).

---

[177] No que tange ao tema, vale destacar que o próprio autor da PEC, o Senador Eduardo Gomes (MDB-TO), refere que a proteção de dados pessoais é uma continuação da proteção da intimidade, sendo que a medida busca assegurar a privacidade desses dados em âmbito constitucional, de modo a resguardar a inviolabilidade das informações dos cidadãos que circulam na *internet*.

Além disso, outro argumento trazido é o de que a PEC dá à proteção de dados tratamento diferenciado, tornando-a praticamente imutável, por depender de um processo mais rígido para mudanças (por meio de emenda à Constituição) do que uma lei ordinária, como a LGPD.

Outro ponto destacado pelo assessor parlamentar do Senado, o advogado Fabricio da Mota Alves, durante a tramitação do projeto de lei que resultou na LGPD, o qual também trabalhou pela inclusão da proteção de dados pessoais na lista dos direitos fundamentais previstos na Consituiçã Federal, é o de que haveria uma separação total da proteção de dados da tradicional discussão sobre privacidade, na medida em que a primeira vai além, sendo muito mais do que mero desdobramento da tutela do direito à privacidade. (LUCA, 2019).

Segundo Bioni (2019, p. 98), “o direito à proteção de dados pessoais angaria autonomia própria. É um novo direito da personalidade que não pode ser amarrado a uma categoria específica, em particular ao direito à privacidade”, ou seja:

> O direito à proteção dos dados pessoais deve ser alocado como uma nova espécie do rol aberto dos direitos da personalidade, dando elasticidade à cláusula geral da tutela da pessoa humana. Caso contrário, corre-se o risco de ele não se desprender das amarras conceituais e da dinâmica do direito à privacidade e, em última análise, inviabilizar uma normatização própria para regular o fluxo informacional como fator promocional da pessoa humana. (BIONI, 2019, p. 100).

Além disso, o assessor parlamentar lembra que muitos outros países com maior experiência que o Brasil na aplicação de leis de proteção de dados pessoais sentiram a necessidade de torná-la um direito fundamental explícito. Nesse sentido, a própria União Europeia fixou a proteção de dados pessoais como direito fundamental a partir da Convenção de Strasbourg, assim como, na América Latina, México e Chile tratam do tema como direito fundamental. (LUCA, 2019).

Frente aos argumentos expostos, entende-se desnecessária a positivação no texto constitucional da proteção de dados pessoais como um direito fundamental autônomo. No caso, é possível extrair da própria noção da privacidade (no sentido do controle sobre os dados) a proteção dos dados pessoais e sensíveis.

Com relação ao ponto, tal conclusão se extrai dos ensinamentos de Schreiber (2013, p. 136-137), segundo o qual:

> O direito à privacidade abrange, hoje, não apenas a proteção à vida íntima do indivíduo, mas também a proteção de seus dados pessoais. Em outras palavras: o direito à privacidade hoje é mais amplo que o simples direito à intimidade. Não se limita ao direito de cada um de ser “deixado só” ou de impedir a intromissão alheia na sua vida íntima e particular. Transcende essa esfera doméstica para alcançar qualquer ambiente onde circulem dados pessoais do seu titular, aí incluídos suas características físicas, código genético, estado de saúde, crença religiosa e qualquer outra informação pertinente à pessoa. Nesse sentido, a privacidade pode ser definida sinteticamente como o direito ao controle da coleta e da utilização dos próprios dados pessoais.

Acrescenta-se, ainda, que muito mais importante do que haver a inclusão expressa no texto constitucional da proteção de dados pessoais como um direito fundamental autônomo, é que esta proteção (agora prevista infraconstitucionalmente, por meio da LGPD) seja observada e garantida. E, no caso, não será a positivação em sede constitucional que ensejará maior ou menor grau de cumprimento, mas a adoção de medidas adequadas e específicas para salvaguardar tal direito.

Avançando para o campo das relações laborais, conforme abordado no capítulo anterior, estas constituem campo propício para a coleta de dados e informações pessoais do trabalhador. Logo, mesmo neste ambiente, a necessidade de proteção aos dados do titular permanece, não se limitando à esfera doméstica, sendo imprescindível compreender a noção de proteção de dados como direito fundamental do trabalhador.

Até porque, não se pode esquecer que o empregado, quando ingressa na relação laboral, traz consigo a condição de pessoa humana titular de direitos fundamentais. Nessa perspectiva:

> [...] a pessoa do trabalhador conjuga os predicados da pessoa que trabalha, que produz trabalho, de modo indissociável e inseparável, portanto, da qualidade ser pessoa humana – esta, inerente a ele. A relação jurídica que envolve os direitos da personalidade alicerça-se a partir da concepção do Direito tendo em primeiro plano a proteção da própria pessoa, do homem. [....] É o elemento humano, como se vê, que justifica a progressividade dos bens tutelados pelos direitos da personalidade, assim considerando todos aqueles que tenham fundamento de existência na preservação da pessoa humana, tal como acontece com a proteção da privacidade da pessoa, ainda que inserida em contexto de relação de emprego. (WEINSCHENKER, 2013, p. 23 e 27).

Portanto, as ações do empregador devem estar pautadas pelo equilíbrio e respeito aos direitos fundamentais da personalidade dos trabalhadores, dentre eles, o da proteção aos dados pessoais e sensíveis destes. Ressalta-se que o próprio direito

à intimidade e à vida privada do trabalhador é um direito inespecífico que, apesar de não estar previsto expressamente no artigo 6º da Constituição Federal como um direito social, tem como destinatário o trabalhador-cidadão. O mesmo raciocínio aplica-se à proteção dos seus dados.

Evidentemente, tal direito não é absoluto, podendo em determinadas situações haver a ponderação, mas desde que observados o devido processo legal, os princípios gerais de proteção e os direitos do titular, garantias estas que ajudam a definir limites ao exercício do tratamento dos dados pelo empregador.

Por fim, fixada a importância da proteção dos dados pessoais e sensíveis como direito fundamental da pessoa-trabalhadora, cabe agora analisar a responsabilidade das empresas na implementação de medidas que assegurem uma tutela adequada aos dados dos seus titulares, o que será objeto do capítulo seguinte.

4 A TUTELA DOS DADOS PESSOAIS E SENSÍVEIS NAS RELAÇÕES LABORAIS: DIREITO DOS TRABALHADORES E ALCANCE DA RESPONSABILIDADE DO EMPREGADOR NO TRATAMENTO DE DADOS

O advento do *Big Data* e das novas tecnologias potencializaram os poderes do empregador, desencadeando a necessidade da construção de um ponto de equilíbrio entre o direito do empregador, de otimizar os resultados com o uso das inovações, e a preservação dos direitos e liberdades fundamentais do trabalhador, em particular, da proteção aos seus dados pessoais e sensíveis, tema objeto da presente pesquisa.

Assim, os principais objetivos deste último capítulo consistem em abordar a tutela dos dados do trabalhador como um direito inespecífico capaz de impor limites ao tratamento dos dados pessoais e sensíveis no âmbito laboral, com enfoque na responsabilidade da empresa no exercício desta atividade.

Para tanto, analisa-se de que forma a Lei nº 13.709/2018, associada à teoria dos direitos fundamentais, bem como os programas de *compliance* de dados no âmbito das empresas, podem contribuir para uma efetiva proteção no tratamento dos dados pessoais e sensíveis do trabalhador brasileiro, desde a fase pré-contratual até depois de findo o pacto laboral entre as partes.

A fim de alcançar tal propósito, questões ainda pouco debatidas no campo laboral, mas que gradativamente ganham relevância no cenário jurídico, como a teoria dos direitos fundamentais como fonte de proteção aos dados pessoais e sensíveis dos trabalhadores, a nova cultura de *compliance* de dados, a responsabilidade das empresas no tratamento dos dados e as políticas e procedimentos previstos na Lei nº 13.709/2018, serão desenvolvidas neste quarto capítulo.

4.1 A TEORIA DOS DIREITOS FUNDAMENTAIS COMO FONTE DE PROTEÇÃO AOS DADOS

Discorre-se cada vez mais sobre a incidência da teoria dos direitos fundamentais nas relações entre particulares,[178] sendo a seara laboral um campo fértil para sua aplicação.[179] No tocante ao tema, Abrantes (2014, p. 133-138) aduz que:

> [...] a eficácia dos direitos fundamentais tem hoje um carácter "natural" no contrato de trabalho, na medida em que é o seu próprio objecto que contém implicitamente uma ameaça para a liberdade do trabalhador. Essa eficácia conduziu, primeiro, à consagração dos direitos fundamentais especificamente laborais, maxime dos direitos colectivos dos trabalhadores, e, posteriormente, ao reconhecimento dos direitos fundamentais não especificamente laborais, direitos da pessoa e do cidadão, que o trabalhador mantém na empresa.

Assim, no Brasil, se por um lado a Constituição Federal garante o direito ao livre exercício da atividade econômica (artigo 170), da mesma forma, as ações do empregador devem estar pautadas pelo equilíbrio e respeito aos direitos fundamentais da personalidade dos trabalhadores, dentre eles, o direito fundamental à proteção dos dados pessoais e sensíveis, tema objeto da presente pesquisa.

É preciso lembrar que as relações de trabalho caracterizam-se pela longa duração e pelo grande fluxo informacional, o qual se inaugura muito antes da fase contratual. Logo, não só o volume, mas a própria atividade de tratamento dos dados pessoais passa a ser atingida pelo progresso da ação temporal, permeada pela crescente inovação tecnológica.

Consequentemente, não há como prever todas as situações envolvendo o tratamento dos dados no âmbito laboral, pois com o surgimento das novas funcionalidades, outros elementos serão ajustados com o desenrolar das relações, sendo inviável fixar de antemão todas as circunstâncias em que a atividade de tratamento será permitida ou não.

Isso não significa que o empregador tenha ampla permissão para, em nome dos direitos constitucionais de propriedade e da liberdade contratual, realizar o

---

[178] Amaral (2015) observa que no início não se imaginava razão para serem aplicados os direitos fundamentais nas relações entre os privados. Porém, com o tempo se percebeu que, apesar de haver uma igualdade formal, as relações jurídicas na sociedade comportam situações que não guardam uma igualdade material, havendo necessidade da aplicação dos direitos fundamentais a todos os setores do ordenamento jurídico. Assim, verificado que o perigo não se encontra apenas na esfera pública, mas que poderes sociais e indivíduos são capazes de ameaçar e causar danos aos direitos fundamentais, surgiu a vinculação dos particulares a essa categoria de direitos, o que se costumou denominar como "eficácia horizontal dos direitos fundamentais".

[179] Refere-se que a eficácia horizontal dos direitos fundamentais (*Drittwirkung)* foi pela primeira vez abordada na Alemanha, em meados do século XX (1950), em um caso envolvendo a igualdade salarial da mulher no âmbito das relações de trabalho, o qual preconizava "igual salário para mulheres de mesma performance". (AMARAL, 2015).

tratamento dos dados daqueles que lhe prestam serviço. Pelo contrário, as variantes de tratamento dos dados pessoais e sensíveis devem estar adequadas ao contexto da relação.

Assim, a aplicabilidade dos direitos deve ocorrer de forma harmônica e equilibrada, de acordo com os princípios de um Estado Social e Democrático de Direito, de modo que as normas inerentes ao tratamento dos dados não inviabilizem o desenvolvimento da atividade empresarial, mas também não aumentem a deficiência da posição jurídica ocupada pelo trabalhador, resultante da assimetria existente entre as partes.

A relação laboral, como abordado no capítulo 02, é marcada pela chamada subordinação, na qual o empregador detém o poder de emitir diretrizes, instruções ou pedidos que considere convenientes para obter os objetivos da empresa, cabendo ao trabalhador a obrigação de cumprir tais disposições ao longo da prestação de seu trabalho.

Assim, o empregador figura como detentor do chamado poder de direção e disciplina, isto é, da faculdade de dirigir e manter a ordem dentro da empresa, que é uma decorrência da manifestação dos direitos constitucionais de propriedade e liberdade para o desenvolvimento da atividade econômica. Em contrapartida, há igualmente outros direitos fundamentais que podem se opor àqueles direitos constitucionais.

No caso específico, menciona-se o direito fundamental à proteção dos dados pessoais e sensíveis do trabalhador, cuja tutela não é absoluta, estando sujeita a limitações quando colide com outros direitos, como por exemplo, a liberdade de contratação, de gestão e de organização empresarial.[180] Dessa forma:

> A subordinação jurídica no âmbito da relação laboral, quando confrontada com a utilização das tecnologias e com o tratamento de dados pessoais do trabalhador, deve ser adequada às exigências legais atinentes ao regime de proteção de dados, assumindo particular relevância, nomeadamente os princípios do fim, da adequação, da necessidade e da proporcionalidade, da

[180] Em outras palavras, “não pode esquecer-se que existem dois interesses contrapostos: o do trabalhador, cioso de proteger os seus direitos e liberdades, e do empregador, desejoso de conhecer todos os elementos suscetíveis de terem uma influência sobre o funcionamento da empresa. Para resolver esta contraposição de interesses propendemos para considerar que o critério que deve ser seguido é o da boa fé, atendendo ao direito à privacidade que é assegurada a todos os trabalhadores e também candidatos. Na verdade, os direitos fundamentais não podem ficar extramuros, do lado de fora da empresa, impondo-se perante entidades públicas mas também entre privados, onde se inserem os sujeitos da relação de trabalho.” (MOREIRA, 2016, p. 43).

> transparência e da boa-fé, como os direitos de informação, acesso e oposição. (CNPD, 2013, p. 03).

Ao lado da teoria da eficácia horizontal dos direitos fundamentais, a boa-fé (objetiva), como já referido[181], não por acaso é o primeiro princípio expressamente previsto na LGPD a ser observado como guia nas atividades envolvendo tratamento de dados pessoais:

> Os princípios da boa-fé e da confiança estão entrelaçados e detêm uma relação de complementariedade um para com o outro. É do dever de cooperação, lealdade, enfim, de uma conduta proba (boa-fé), que se extraem situações de confiança que devem ser tuteladas.
> [...]
> A privacidade contextual reside justamente na fidelidade depositada pelo emissor de uma informação ao(s) seu(s) recipiente(s), na legítima expectativa de que seus dados pessoais serão usados e compartilhados de acordo com o contexto de uma relação preestabelecida ou a razão pela qual foi publicizado um dado; particularmente, na esperança de que o trânsito das suas informações pessoais não minará e trairá a sua capacidade de livre desenvolvimento da personalidade e de participação social. (BIONI, 2019, p. 247).

Quanto à eficácia horizontal dos direitos fundamentais, a incidência desta teoria contribui como limite a ser observado pelo responsável pelo tratamento dos dados pessoais e sensíveis do trabalhador, entendido este como um novo direito de personalidade da pessoa trabalhadora.[182] A existência de limites é de extrema importância, pois as relações laborais caracterizam-se pelas relações desiguais, "quer no plano factual, quer jurídico, tanto no momento da celebração quanto no da execução do contrato." (ABRANTES, 2014, p. 128).

Portanto, como já adiantado, embora a liberdade empresarial permita que o empregador implemente mecanismos de direção e controle sobre os trabalhadores, o que inclui operações realizadas com os seus dados pessoais, como as que se

---

[181] Remete-se o leitor ao item 3.3.

[182] Como já mencionado nos capítulos anteriores, os direitos de personalidade não se limitam às espécies enumeradas nos artigos 11 a 21 do Código Civil. Nesse sentido, o Enunciado nº 274 da IV Jornada de Direito Civil: "Os direitos da personalidade, regulados de maneira não-exaustiva pelo Código Civil, são expressões da cláusula geral de tutela da pessoa humana, contida no art. 1º, inc. III, da Constituição (princípio da dignidade da pessoa humana). Em caso de colisão entre eles, como nenhum pode sobrelevar os demais, deve-se aplicar a técnica da ponderação. (CJF, 2006). Da mesma forma, no caso da pessoa-trabalhadora, os direitos de personalidade, extraídos a partir do artigo 223-C da CLT, que cuida dos bens extrapatrimoniais do trabalhador juridicamente tuteláveis, configuram um rol meramente exemplificativo. (GOLDSCHMIDT, 2019b). Assim, dada a elasticidade e a abertura para o reconhecimento de novos direitos, é possível identificar uma nova variante desta categoria jurídica para nela enquadrar a proteção dos dados pessoais como um novo direito da personalidade.

referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração, é preciso que tais ações decorrentes do poder empregatício estejam em consonância com os direitos fundamentais do trabalhador, devendo ser aplicadas proporcionalmente.[183]

Não se pode esquecer, ainda, que:

> O contrato de trabalho, porque implica o envolvimento integral do trabalhador, aumentando a probabilidade de ameaças aos seus direitos fundamentais enquanto pessoa humana, representou, desde sempre, por toda a parte, nos ordenamentos democráticos, o âmbito natural para o desenvolvimento de uma tal eficácia dos preceitos e valores constitucionais, tornando-se necessário responder à questão de saber *se – e até que ponto –* os interesses na base do poder do empregador exigem e justificam, no caso concreto, a limitação da liberdade do trabalhador. (ABRANTES, 2014, p. 143).

Contudo, importante ressaltar que, quando se fala em proteção de dados, não se tem:

> [...] por objetivo inviabilizar a coleta de dados para conhecimento do público alvo e aprimoramento das atividades empresariais. Todo empresário tem legítimo interesse de conhecer quem são seus consumidores, empregados e candidatos a emprego. Entretanto, a LGPD esclarece que os dados coletados para essa finalidade legítima pertencem às pessoas físicas às quais os dados se referem e precisam ser tratados e coletados em respeito a essa relação de pertencimento. (FRAZÃO; OLIVA; ABILIO, 2019, p. 696).

Assim, o direito fundamental à proteção de dados pessoais só pode ser limitado ou restringido por outro direito de igual hierarquia. A própria OIT, por meio do Repertório de Recomendações Práticas sobre a Proteção de Dados, limita o legítimo interesse[184] dos empregadores no tratamento de dados pessoais de trabalhadores em

---

[183] Quanto ao tema, Abrantes (2014) explica que a eficácia dos direitos fundamentais da pessoa humana no âmbito da relação de trabalho é passível de limitação pelos "interesses legítimos" do empregador ou de terceiros. O autor (2014, p. 168) "aponta para um critério de concordância prática entre a liberdade civil do trabalhador e a autonomia contratual, através de um *princípio de proporcionalidade*, na sua tripla dimensão de *necessidade* (de salvaguardar a correcta execução do contrato), de *adequação* (entre o objectivo a alcançar com a limitação e o nível desta) e de *proibição do excesso* (devendo a restrição ser a menor possível, em função da finalidade a ser alcançada com a sua imposição).

[184] Segundo Bioni (2019, p. 248-249), "historicamente, o legítimo interesse tem sido encarado como a mais flexível das bases legais de tratamento de dados no regime do direito comunitário europeu." A referida base legal "ganhou ainda mais relevância diante da emergência de tecnologias e no contexto de uma economia baseada no uso intensivo de dados. [...] ganhou o *status* de uma nova 'carta coringa regulatória' para abraçar uma miríade de possíveis usos dos dados." A antiga diretiva europeia de

aspectos estritamente necessários[185], como o perfil para a seleção de candidatos, a formação e promoção de pessoal, a salvaguarda da segurança pessoal e do trabalho e o controle de qualidade nas atividades realizadas. (OIT, 1997).

Apesar desses avanços, as evidências indicam que eles foram insuficientes e, em muitos casos, limitados frente a cenários laborais complexos.

Em face disso, ganha relevo o chamado teste de proporcionalidade do legítimo interesse, pois não se pode conceber que o empregador trate dados de diferentes tipos, que muitas vezes violam o respeito à esfera individual do empregado, sob pena de configurar um retorno dos trabalhadores aos abusos a que foram submetidos antes da existência do Direito do Trabalho. Nesse sentido:

> Os direitos do trabalhador constituem limites ao exercício dos poderes patronais e o seu exercício só pode ser restringido se e na medida em que colidir com interesses relevantes do empregador, ligados ao bom funcionamento da empresa e ao correcto desenvolvimento das prestações contratuais.
> As restrições a esses direitos devem "*limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos*" (por exemplo, a honra ou reserva de intimidade do empregador e dos outros trabalhadores, o direito à saúde e à integridade física e moral, a liberdade de empresa e a propriedade privada, etc.), devendo, além disso, apenas ir até onde não afectem "*a extensão e o alcance do conteúdo essencial*" dos direitos em questão [...]. (ABRANTES, 2014, p. 179).

Assim, o chamado teste de proporcionalidade do legítimo interesse, à semelhança do que consta no RGPD, prevaleceu na LGPD[186], consistindo no

---

proteção de dados não detalhava os critérios para a aplicação do legítimo interesse. Foi o Grupo de Trabalho do artigo 29 que formulou uma opinião sobre legítimo interesse ao estabelecer critérios para a sua aplicação, com o objetivo de trazer previsibilidade e segurança jurídica na aplicação dessa base legal em todo o bloco econômico europeu e evitar que fosse um 'porta aberta' para contornar os direitos e princípios da diretiva. O RGPD, em particular no considerando 47, também internalizou o vocabulário prescrito na referida opinião sobre legítimo interesse. (UNIÃO EUROPEIA, 2016). No cenário interno, a LGPD brasileira previu o legítimo interesse no rol das hipóteses legais para o tratamento de dados pessoais, o que se extrai da leitura do artigo 10 da Lei nº 13.709/2018. (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

[185] Em igual sentido, a LGPD, em seu artigo 6º, inciso III, ao tratar do princípio da necessidade, demarca alguns limites ao tratamento de dados ao estabelecer que este deve se restringir ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados. (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

[186] Destaca-se que além da hipótese do legítimo interesse do controlador ou de terceiro, o artigo 7º da LGPD menciona outras hipóteses em que o tratamento dos dados pessoais poderá ser realizado, tais como: mediante o fornecimento de consentimento pelo titular, para o cumprimento de obrigação legal, pela administração pública, para a execução de políticas públicas, para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais, para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, para o exercício regular de direitos em processo judicial, administrativo ou arbitral, para a

balanceamento dos interesses do titular dos dados (posição ocupada pelo trabalhador) e dos agentes de tratamento de dados pessoais (posição ocupada pelo empregador ou por quem realiza o tratamento em seu nome).

Diante disso, “tão importante quanto aferir se há um *interesse legítimo* é verificar se as *legítimas expectativas* e os direitos e liberdades fundamentais do cidadão [trabalhador] serão respeitados.” Contudo, tal tarefa não é nada fácil, pois os “dois principais componentes dessa difícil equação são conceitos jurídicos indeterminados (legítimo interesse[187] e legítima expectativa[188]), o que a torna ainda mais complexa.” (BIONI, 2019, p. 252).

Assim, com fundamento na opinião do Grupo de Trabalho do artigo 29 – GT29 popularizou-se um teste composto de quatro fases para a aplicação do legítimo interesse para o tratamento de dados: [189]

> [...] não se trata de um teste da ponderação simples, que consiste apenas em ponderar dois ‘valores’ facilmente quantificáveis e facilmente comparáveis em relação um ao outro. Pelo contrário, [...] aplicar o teste da ponderação pode exigir uma avaliação complexa que tenha em conta vários fatores. Para ajudar a estruturar e a simplificar a avaliação, dividimos o processo em várias

proteção da vida ou da incolumidade física do titular ou de terceiro, para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária, ou, ainda, para a proteção do crédito. (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

[187] O GT29 associa o conceito de ‘interesse’ ao conceito de ‘finalidade’. “Em matéria de proteção de dados, a ‘finalidade’ é a razão específica pela qual os dados são tratados: o objetivo ou a intenção do tratamento de dados. Por outro lado, um interesse é o objetivo mais abrangente que o responsável pelo tratamento pode ter no tratamento, ou o benefício que o responsável pelo tratamento retira – ou que a sociedade pode retirar – do tratamento.” No caso, “uma empresa pode ter um *interesse* em garantir a saúde e a segurança do seu pessoal que trabalha na sua unidade de produção de energia nuclear. Neste sentido, a empresa pode ter como *finalidade* a implementação de procedimentos específicos de controlo de acessos que justifique o tratamento de determinados dados pessoais definidos como forma de garantir a saúde e a segurança do pessoal.” Segundo o GT29, “um interesse deve ser definido de forma suficientemente clara para permitir a realização do teste da ponderação em relação aos interesses e aos direitos fundamentais da pessoa em causa. Além disso, o interesse em jogo deve ser igualmente ‘do responsável pelo tratamento’. Tal exige que se trate de um interesse real e atual, algo que corresponda a atividades atuais ou a benefícios esperados num futuro muito próximo. Por outras palavras, os interesses que sejam demasiado vagos ou especulativos não serão suficientes.” E quanto ao interesse ser legítimo ou ilegítimo, “o conceito de interesse legítimo pode incluir um vasto leque de interesses, sejam eles triviais ou muito preponderantes, simples ou mais controversos. Por conseguinte, só num segundo momento, quando se trate de ponderar esses interesses em relação aos interesses e aos direitos fundamentais da pessoa em causa, deve ser adotada uma abordagem mais restrita e uma análise mais substancial.” (GT29, 2014b, p. 38-40).

[188] O GT29 utiliza a terminologia ‘expectativas razoáveis da pessoa em causa’, o qual relaciona-se com as expectativas razoáveis quanto ao que acontecerá aos dados do titular, bem como a natureza deles e a forma como serão tratados. (GT29, 2014b).

[189] De acordo com o GT29, as quatro fases são: a) avaliação do interesse legítimo do responsável pelo tratamento, b) impacto nas pessoas em causa, c) equilíbrio provisório e d) garantias complementares aplicadas pelo responsável pelo tratamento para evitar qualquer impacto indevido nas pessoas em causa. (GT29, 2014b).

> fases, de forma a assegurar que o teste da ponderação possa ser realizado de forma eficaz. (GT29, 2014b, p. 37).

Com base no chamado teste de ponderação, Bioni (2019), apresenta o teste de proporcionalidade, previsto na LGPD, como necessário para a promoção do tratamento dos dados pessoais com base no legítimo interesse. Desse modo, a partir de uma interpretação sistemática entre o artigo 6º, inciso X, e os artigos 10 e 37, todos da LGPD, o autor (2019) descreve o referido teste por meio das suas etapas.

A primeira delas diz respeito à verificação da *legitimidade do interesse: situação concreta e finalidade legítima* (artigo 10, *caput* e I, da LGPD). Nesta fase, o primeiro passo é verificar se o interesse do controlador é legítimo (finalidade legítima), isto é, senão contraria outros comandos legais, como, por exemplo, no caso da vedação de coleta de dados, mesmo com o consentimento do seu titular nas relações de trabalho, relacionados à gravidez, AIDS/HIV e toxicológico (Portarias nº 1.246/2010 e 41/2007). O que importa aqui é observar se há algum benefício ou vantagem com o uso dos dados por parte do controlador e não do titular dos dados. A partir disso, deve-se verificar se o interesse está claramente articulado, para que não seja um cheque em branco. Assim, “quanto mais bem definida e articulada tal situação, mais fácil será analisar o legítimo interesse diante dos próximos três passos, diminuindo os riscos de ser considerado como algo meramente especulativo." (BIONI, 2019, p. 253).

A segunda etapa refere-se à *necessidade: minimização e outras bases legais* (artigo 10, § 1º, da LGPD). Tem por objetivo verificar se os dados coletados são realmente aqueles necessários (minimização) para se atingir a finalidade pretendida. Ou seja, apura-se se seria possível atingir o mesmo resultado por meio de uma quantidade menor de dados, de modo a ser menos intrusivo e impactando menos a pessoa em causa. Além disso, verifica-se se o tratamento dos dados não seria coberto por outras bases legais, que não a do interesse legítimo. (BIONI, 2019).

O *balanceamento: impactos sobre o titular dos dados e legítimas expectativas* (artigo 10, II, da LGPD) corresponde à terceira etapa. Trata-se da principal fase do teste de proporcionalidade, na qual são sopesados os interesses das partes (do controlador e de terceiros diante do titular dos dados). Apura-se se o novo uso atribuído ao dado está dentro das legítimas expectativas do titular, o que é parametrizado pela noção de compatibilidade entre o uso adicional e aquele que originou a coleta dos dados pessoais. Para Bioni (2019, p. 254-255), “eles devem ser próximos um do outro, demandando-se uma análise *contextual* para verificar se esse

uso secundário seria esperado pelo titular dos dados." Somado a isso, deve-se verificar de que forma eles são impactados, especialmente repercussões negativas em termos de discriminação e sobre a sua autonomia.

No tocante ao tema, Bioni (2019) ressalta que a maior dificuldade da aplicação do legítimo interesse ocorre quando envolve terceiros (alguém que não mantém uma relação já preestabelecida com o titular dos dados), isso porque, nesses casos, a noção de legítima expectativa é mais complicada de ser demonstrada e o risco da aplicação dessa base legal é ainda maior.

A última fase refere-se às *salvaguardas: transparência e minimização dos riscos ao titular do dado* (artigo 10, §§ 2º e 3º, da LGPD). Em tal fase, destaca-se o dever de transparência, por meio do qual objetiva-se franquear à pessoa em causa "o poder de tomada de decisão para se opor a tal atividade de tratamento de dados (*opt-out*), podendo optar por estar fora do que considera ser incompatível com as suas legítimas expectativas." (BIONI, 2019, p. 255). Associado a isso, o controlador deve adotar ações para mitigar os riscos ao titular dos dados (como, por exemplo, a anonimização dos dados).

Apresentado o teste de proporcionalidade, há diversos casos práticos, a partir dos quais é possível aplicar o referido teste. Dentre eles, para a presente análise, destaca-se uma iniciativa cada vez mais comum entre os departamentos pessoais das empresas: a reunião de informações sobre candidatos em processos seletivos (prática conhecida como *background-check* ou verificação de antecedentes).

Tal dinâmica tem sido adotada pelas empresas para minimizar os riscos ao desenvolvimento da sua atividade. A prática do *background-check* inicia com a habilitação do candidato a uma vaga de trabalho[190]. A partir de então, o contratante, com base nos dados contidos no currículo, verificará o seu histórico como forma de checar as competências declaradas e a adequação de seu perfil para a vaga, o que pode incluir verificação de antecedentes criminais, comerciais, financeiros, histórico

[190] Sobre a fase de acesso ao emprego, considera-se este o momento em que "o trabalhador-candidato se encontra mais fragilizado já que é nessa altura que a desigualdade real mais se evidencia, concretizada numa inferioridade pré-contratual do candidato. [...] Na verdade, parece ser nesta fase que se podem produzir as violações mais flagrantes da lei e dos direitos fundamentais dos trabalhadores e, por isso mesmo, é necessária uma maior vigilância e proteção de possíveis intromissões na vida privada do candidato. Este, com receio de ser excluído do processo de seleção, disponibilizar-se-á para mencionar dados e factos da sua vida pessoal, operando uma *limitação voluntária* de um direito de personalidade [...] e, por isso, livremente revogável, que excede muitas vezes o razoável e necessário para o conhecimento da sua aptidão para o posto de trabalho em causa." (MOREIRA, 2016, p. 36).

de processos e ações trabalhistas diante de outras empresas e, até mesmo, navegação pelas redes sociais[191].

Aplicando-se o teste de proporcionalidade à situação hipotética, é possível percorrer as quatro etapas para avaliar o balanceamento entre a promoção da atividade do empregador e os direitos e liberdades fundamentais do candidato à vaga.

Quanto à primeira fase, correspondente à *legitimidade*, inegável que o empregador (ou terceiro por ele contratado) tem um interesse legítimo em acumular elementos para auxiliar e respaldar a sua decisão. Tal investigação se justifica por atribuir maior eficiência e precisão aos processos seletivos, sendo um apoio para o desenvolvimento das atividades.

Na segunda fase, relacionada à *necessidade*, dada a assimetria existente entre as partes na relação laboral, tem-se que o consentimento nem sempre servirá como elemento legitimador para o tratamento dos dados, conforme abordado no capítulo 3.[192] Em razão disso, o legítimo interesse se apresentaria como uma possível base legal, pois a reunião de informações sobre candidatos em processos seletivos é uma das formas de o empregador exercer o seu poder diretivo sobre aqueles que lhe prestam serviço ou almejam tal posição.

Contudo, a dúvida que surge e que seria a mais controvertida de todas é sobre quais são os dados necessários para avaliar o candidato, ou seja, "o que poderia ser enquadrado como uma informação útil para compor o quadro analítico das habilidades e técnicas do candidato ao exigido pela vaga".[193] (BIONI, 2019, p. 262).

---

[191] Assim, os empregadores "podem, ainda, na fase de seleção, consultar a informação que os candidatos colocam nas redes sociais ou nos seus *blogs* pessoais e excluí-los de acordo com o conteúdo dessa informação." Ou seja, tais redes "possibilitam ainda que quem é responsável pelo recrutamento analise os currículos e informações pessoais e profissionais dos candidatos. (MOREIRA, 2016, p. 17 e 19). Para maior aprofundamento do uso das redes sociais pelas empresas na fase pré-contratual, remete-se o leitor ao item 2.4.

[192] Para maior aprofundamento do tema do consentimento nas relações laborais, remete-se o leitor ao item 3.2.

[193] A propósito do tema, no julgamento de incidente de recurso repetitivo (IRR-243000-58.2013.5.13.0023), a Subseção 1 Especializada em Dissídios Individuais (SDI-1) decidiu que as empresas não podem exigir certidão de antecedentes criminais de candidatos a emprego, salvo em situações excepcionais. Nesse sentido, foram fixadas as seguintes teses: 1. Não é legítima, e caracteriza lesão moral, a exigência de certidão de antecedentes criminais de candidato a emprego quando traduzir tratamento discriminatório ou não se justificar em razão de previsão em lei, da natureza do ofício ou do grau especial de fidúcia exigido. 2. A exigência de certidão de candidatos a emprego é 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 e pessoas com deficiência, em creches, asilos ou instituições 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 e entorpecentes e armas, trabalhadores que atuam com informações sigilosas.

Quanto ao *balanceamento*, é esperado que em um cenário envolvendo processo seletivo “haja algum tipo de confirmação ou investigação das informações, habilidades e técnicas declaradas pelo candidato. Ou seja, está dentro das suas legítimas expectativas que haja tal tipo de tratamento de dados”. No balanceamento, o ponto “parece ser a prevenção de práticas discriminatórias injustificadas.” (BIONI, 2019, p. 262).

No caso, é preciso lembrar que o trabalho, além de ser um direito social (artigo 6º da CF) é também um dos princípios fundamentais da República Federativa do Brasil (artigo 1º, IV, da CF), de modo que a prática do *background-check* deve ser prudente para que não configure mais um obstáculo no acesso ao mercado de trabalho.

Quanto à última etapa do teste, a *salvaguarda* relaciona-se ao dever de transparência e minimização dos riscos ao titular do dado. Assim, fundamental que a empresa haja segundo os ditames da boa-fé e da transparência, evitando surpreender o candidato com atos patronais não comunicados. Daí a importância de informar sobre a prática do *background-check* logo no início da seleção.

Diante disso, a fim de garantir uma harmonia entre o valor social da proteção dos dados pessoais e sensíveis do trabalhador e o valor social da propriedade privada:

> [...] O empregador, além de realizar o teste de ponderação, deverá: garantir que seja realizado um tratamento legítimo e específico dos dados do trabalhador. Considerar os princípios de minimização. Aplicar princípios de proporcionalidade e subsidiariedade. Procedimentos transparentes no uso de novas tecnologias. Permitir que os trabalhadores exerçam seus direitos sobre o tratamento de dados pessoais.[194] (GIMÉNEZ, 2019, p. 05, tradução nossa).

---

3. A exigência da certidão de antecedentes criminais, quando ausentes alguma das justificativas de que trata o item 2, caracteriza dano moral *in re ipsa* [presumido], passível de indenização, independentemente de o candidato ao emprego ter ou não sido admitido. (TST, 2017). Contudo, o Tribunal Superior do Trabalho “acabou por trazer um rol bastante amplo de situações nas quais seria justificável o uso de tais informações. Com a LGPD, é muito provável que tais questões voltem à tona, oxigenadas pela aplicação desse teste de proporcionalidade”. (BIONI, 2019, p. 262).

[194] *El empresario además de realizar el juicio de ponderación deberá: Asegurarse de que se realiza un tratamiento legítimo y específico de los datos del trabajador. Considerar los principios de minimización. Aplicar principios de proporcionalidad y subsidiariedad. Procedimientos transparentes en el uso de nuevas tecnologías. Permitir a los trabajadores ejercer sus derechos sobre el tratamiento de datos personales*.

A não observância dos limites e garantias constitucionais coloca em perigo os dados pessoais dos seus titulares, podendo afetar o desenvolvimento da personalidade do trabalhador. Um tratamento sem freios, intermediado pelos dados, torna a pessoa-trabalhadora um ser passível de exploração ilimitada.

Daí a importância de, ao lado da teoria dos direitos fundamentais como fonte de proteção aos dados pessoais e sensíveis do trabalhador, investir-se na construção de uma cultura que permita a adoção do *compliance* de dados no ambiente laboral, questão objeto do próximo ponto.

4.2 A NOVA CULTURA DE *COMPLIANCE* EM MATÉRIA DE PROTEÇÃO DE DADOS E SUA ADOÇÃO NO ÂMBITO LABORAL

Na era digital, um dos grandes desafios que surge nas relações entre empregador e trabalhador consiste em como processar as informações de cunho pessoal sem comprometer o direito fundamental dos trabalhadores a uma eficaz e efetiva proteção de dados pessoais, na medida em que “a gestão da informação sobre si próprio tornou-se expressão fundamental do indivíduo.” (FRAZÃO; OLIVA; ABILIO, 2019, p. 678).

Com efeito, frente à relevância do tema, a OIT, em 1997, ao aprovar o Repertório de Recomendações Práticas em matéria de proteção de dados pessoais dos trabalhadores, dispôs no item 5.11:

> Os empregadores, os trabalhadores e seus representantes devem cooperar na proteção de dados pessoais e na elaboração de uma política de empresa que respeite a vida privada dos trabalhadores, de acordo com os princípios estabelecidos neste repertório.[195] (OIT, 1997, p. 02, tradução nossa).

Percebe-se, portanto, que uma das ações indicadas pela OIT para a tutela dos dados pessoais e sensíveis dos trabalhadores consiste, em outras palavras, na implementação dos chamados programas de *compliance*, os quais correspondem à noção de “conformidade com a legislação do Estado e com as demais normas de

---

[195] *Los empleadores, los trabajadores y sus representantes deberían cooperar en la protección de los datos personales y en la elaboración de una política de empresa que respete la vida privada de los trabajadores, con arreglo a los principios enunciados en el presente repertorio*.

conduta que possam ser aplicáveis às pessoas de determinada organização." (ANDRADE, 2017, p. 76). Assim, o termo corresponde:

> [...] à adesão da companhia a normas ou procedimentos de determinado setor. Seu objetivo primordial é o combate à corrupção. Diferentemente da ética, que é assumida com espontaneidade, o *compliance* está relacionado à responsabilidade legal [...]. Ser ético é agir voluntariamente com princípios morais para com a sociedade. Já *compliance* é cumprir com regras e regulamentos; é trabalhar ou agir dentro da lei. [...] Formado por leis, decretos, resoluções, normas, atos e portarias, o *compliance* é todo arcabouço regulatório aplicado pelas agências que controlam e regulam o setor no qual a empresa está inserida. As maiores e mais organizadas corporações também criam suas próprias normativas internas para direcionar o comportamento de seus diretores e executivos e, assim, coibir comportamentos negativos, desvios de conduta e inconformidades. (ANTONIK, 2016, p. 976 e 987).

Ou seja, o *compliance* cuida:

> [...] da estruturação de políticas e procedimentos corporativos que se traduzam em ações sistemáticas com o objetivo de atender ao cumprimento aos preceitos normativos, a permitir a prevenção do ato ilícito ou, caso tal não seja possível, minorar seus efeitos e sancionar eventuais responsáveis. (FRAZÃO; OLIVA; ABILIO, 2019, p. 683-684).

No Brasil, o instituto ganhou relevo após os escândalos de corrupções políticas, tendo como marco principal a Lei Anticorrupção[196] ou Lei do *Compliance*, cujo instrumento normativo dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas, de qualquer natureza ou formato societário, pela prática de atos contra a administração pública nacional ou estrangeira.

Assim, o *compliance*, também conhecido como programa de comprometimento ou programa de integridade[197], emergiu "como uma necessidade imposta pela sociedade em direção às empresas, de forma a exigir maior transparência e seriedade nas relações negociais." (LAZZARIN; CAVAGNOLI, 2018, p. 99).

Em um primeiro momento, prevaleceu o entendimento de que tais programas seriam apenas um mecanismo para minimizar a aplicação de sanções

---

[196] Lei n° 12.846, de 1° de agosto de 2013.

[197] O Decreto nº 8.420/2015, de 18 de março de 2015, que regulamenta a Lei nº 12.846/2013, disciplinou em seu artigo 41 os programas de integridade para designar os programas de *compliance*. Cabe, ainda, destacar a recente publicação do Decreto nº 9.751, de 21 de novembro de 2018, que estabelece as diretrizes nacionais sobre empresas e direitos humanos, o qual também prevê em seu artigo 10 a criação e manutenção de programas integridade.

penais contra empresas e organizações privadas que praticassem atos de corrupção ao realizarem negócios com a Administração Pública.[198]

Apesar disso, a adoção do instituto não se ateve ao campo penal, pois o programa não se limita ao combate à corrupção, uma vez que há falhas que podem ser muito mais danosas para uma empresa, razão pela qual deve incluir áreas como a antitruste, tributária, ambiental, propriedade intelectual, trabalhista[199], assim como todos os campos suscetíveis a erros.

No caso específico da proteção de dados:

> Diante da facilidade e imediatismo do compartilhamento de informações, pela exposição de conteúdos, privacidade e imagens, inegavelmente, há constante preocupação com a gestão dos riscos e danos decorrentes dessas atividades. (BLUM; ZAMPERLIN, 2016).

Dessa maneira, frente ao atual cenário marcado, por um lado, pelas alterações na lógica até então vigente quanto ao tratamento de dados e, por outro, pela necessidade de se conferir papel primordial na efetividade dos direitos e na prevenção de danos:

> [...] a adoção de mecanismos de *compliance* consubstancia valioso instrumento desse viés operacional e preventivo, auxiliando na promoção de condutas compatíveis com a regulamentação legal. No âmbito da proteção de dados pessoais, [...] seja por seu inerente dinamismo, seja por haver diversas lacunas para se viabilizar o cumprimento dos preceitos legais, o papel das ações dos agentes econômicos robustece-se ainda mais. A implementação de boas práticas no tratamento de dados pessoais possui estrondoso potencial para auxiliar no atendimento aos comandos gerais da lei de acordo com as particularidades de determinados agentes econômicos, bem como prevenir a ocorrência de violações aos direitos dos titulares, na medida em que permite orientar os agentes de tratamento, traduzindo para suas atividades cotidianas as premissas principiológicas da LGPD e concretizando vários dos seus *standards* e conceitos abertos. (FRAZÃO; OLIVA; ABILIO, 2019, p. 682).

---

[198] Tal noção se explica, na medida em que a origem dos programas de *compliance* remonta ao ano de 1977, quando o Governo dos Estados Unidos da América promulgou o *Foreign Corrupt Practices Act* (FCPA), momento em que o pano de fundo era o escândalo de corrupção conhecido como *Watergate*. (MUNIZ; DIAS, 2016, p. 530).

[199] Na seara laboral, embora inexista uma lei específica sobre *compliance*, a sua implementação deve nortear-se pela legislação trabalhista, pela observância dos direitos de personalidade do trabalhador, pela adesão às práticas de governança corporativa, pela criação de um código de ética ou código de conduta, pelo oferecimento de treinamento aos trabalhadores para melhor desempenho de suas funções, pela implementação de canais de denúncia, dentre outras. (LAZZARIN; CAVAGNOLI, 2018).

Assim, em matéria de proteção de dados, o caráter complementar das políticas de *compliance* têm grande serventia, isso porque:

> [...] a LGPD apresenta grande plasticidade, utilizando-se de diversos *standards* e conceitos abertos, que precisam ser necessariamente contextualizados diante da realidade de cada agente econômico, do contexto social e econômico e da evolução tecnológica do momento em que forem aplicados. Logo, é fundamental que, ao lado do papel regulamentador da autoridade nacional, os agentes econômicos possam também ter a iniciativa de dar concretude aos comandos legais, adaptando-os à sua realidade a partir dos incentivos e dos esclarecimentos que recebem do próprio Estado. (FRAZÃO; OLIVA; ABILIO, 2019, p. 685).

A propósito, o artigo 50 da LGPD, ao tratar das boas práticas e da governança, previu a implementação de programas de *compliance*, aos quais denominou de programas de governança em privacidade, nos seguintes termos:

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.
> § 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.
> § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:
> I – implementar programa de governança em privacidade que, no mínimo: a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais; b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta; c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados; d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade; e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular; f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos; g) conte com planos de resposta a incidentes e remediação; e h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;
> II – demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou

> códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei. (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).[200]

Portanto, o *compliance* na LGPD, além de permitir a prevenção, funciona como um instrumento de contenção de riscos, na medida em que a empresa que o adota se compromete a cumprir o ordenamento jurídico e as imposições dos órgãos de regulamentação, dentro dos padrões exigidos para o seu segmento de atuação.

Contudo, embora o programa represente um passo importante para o tratamento de dados, para que as suas vantagens[201] sejam efetivamente materializadas, são elencados dez elementos mínimos que caracterizam um programa de *compliance* robusto, sendo estes aplicáveis ao *compliance* de dados no âmbito laboral. (FRAZÃO; OLIVA; ABILIO, 2019).

O primeiro deles refere-se à *avaliação contínua de riscos e atualização do programa*. De acordo com este elemento, deve-se avaliar os riscos a que se submete a empresa (levando em consideração as suas peculiaridades, tais como a complexidade e a estrutura da organização). Com isso será possível elaborar um programa de *compliance* personalizado que efetivamente se contraponha aos pontos mais sensíveis para a entidade.

Em se tratando de *compliance* de dados:

> [...] a noção de tratamento de dados utilizada pela LGPD é ampla, de forma que é difícil se imaginar algum agente econômico que não esteja sujeito à atividade e aos riscos respectivos. Entretanto, o tipo e a intensidade do tratamento de dados, bem como os riscos a ele inerentes, podem variar consideravelmente entre os agentes econômicos, a exigirem uma atenta e

---

[200] Com relação ao dispositivo, o legislador segmenta as regras corporativas em "'regras de boas práticas e de governança' – previstas no *caput* do art. 50 – e o 'programa de governança em privacidade' – previsto exclusivamente para os controladores no § 2º. Enquanto o primeiro parece preocupar-se mais com os aspectos operacionais do processo de tratamento dos dados, de modo a servir como instrumento de definição dos padrões técnicos e dos mecanismos em que se estruturarão o sistema a ser empregado; ao segundo foi conferido escopo mais amplo (como sói acontecer na elaboração das normas de governança corporativa), cogitando-se também das garantias aos titulares dos dados. Em qualquer dos casos, ressalta-se no *caput*, no § 1º e no § 2º o fator risco é primordial. (FRAZÃO; OLIVA; ABILIO, 2019).

[201] São "vantagens tradicionalmente atribuídas aos programas de *compliance* – (i) permitir a adequada gestão do risco da atividade – na medida em que identifica os pontos sensíveis em que há exposição ao descumprimento – e, por consequência, auxiliar na prevenção de ilícitos; (ii) viabilizar a pronta identificação de eventual descumprimento, bem como a remediação de danos daí decorrentes, auxiliando, assim, na minoração dos prejuízos; (iii) fomentar a criação de uma cultura corporativa de observância às normas legais; e (iv) servir potencialmente como atenuante no caso de punições administrativas –, na tutela de dados soma-se à vantagem adicional de adaptar e operacionalizar diversos dos comandos gerais e conceitos abertos da LGPD. Podem-se enumerar, ainda, benefícios, ainda que indiretos, concernentes ao desenvolvimento em qualidade e inovação, além de incrementos reputacionais. (FRAZÃO; OLIVA; ABILIO, 2019, p. 686).

> individualizada análise. Não é sem razão que a própria LGPD já oferece uma importante referência desse tipo de avaliação, ao definir o relatório de impacto à proteção de dados como a 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 (art. 5º, XVII). (FRAZÃO; OLIVA; ABILIO, 2019, p. 687-688).

Portanto, para garantir a efetividade do programa, torna-se fundamental avaliar os riscos envolvidos, bem como reavaliá-los constantemente, atualizando e adaptando as normas internas. Sobre o tema, Pinheiro (2019, p. 320) apresenta as seguintes reflexões:

> [...] a conformidade à proteção de dados é o tipo de projeto contínuo, que exigirá uma revisitação da pauta periodicamente, visto que os negócios estão também em transformação, assim como a tecnologia, trazendo inovação e novas funcionalidades, logo o que é feito hoje sofrerá alterações em curto espaço de tempo e os procedimentos bem como a documentação sobre proteção de dados pessoais, precisará de atualização em intervalos não superiores a dois anos, especialmente no tocante às políticas de privacidade, termos de uso e contratos.
> Logo, ter a lei é apenas o começo de uma longa jornada que teremos que atravessar tanto no âmbito público como privado. Atender aos requisitos da nova lei exige investimento, atualização de ferramentas de segurança de dados, revisão documental, melhoria de processos e, acima de tudo, mudança de cultura.

O segundo elemento corresponde à e*laboração de códigos de ética e conduta*, os quais:

> [...] são acordos que estabelecem direitos e deveres de uma dada corporação e que devem ser respeitados e seguidos por seus colaboradores e demais envolvidos. [...] Recomenda-se que tais códigos estejam em conformidade, ou seja, que estejam em *compliance* com ideais democráticos, a dignidade da pessoa humana, leis trabalhistas, leis ambientais e demais normas pertinentes. No bojo dos códigos de ética torna-se interessante que estejam expressados princípios relacionados à proteção do patrimônio corporativo, à necessária transparência nas comunicações dentro e fora da corporação, ao assédio moral, assédio profissional, assédio sexual e outras formas de assédio, relacionamento interpessoal e parental entre colaboradores, bem como a ações relacionadas à denúncia em caso de práticas de suborno ou corrupção. (CAMARGO; SANTOS, 2019, p. 221-231).

A LGPD incentiva a criação de códigos de ética ou de conduta, de forma a tornar mais efetivo[202] o cumprimento das disposições por parte dos diferentes setores,

---

[202] "Para garantir sua efetividade, tais instrumentos devem fixar deveres expressos e concretos, bem como ser de simples leitura, valendo-se de linguagem clara e direta. Afinal, destinam-se a todos os setores da pessoa jurídica e, sem que seus funcionários sejam capazes de compreender os preceitos

tendo em consideração as suas especificidades, bem como a certificação[203] na área da proteção de dados e de selos de proteção. [204]

O terceiro elemento diz respeito à organização compatível com o risco da *atividade*. Ou seja, o programa deve ser estruturado, aplicado e atualizado de acordo com as características e riscos das atividades de cada pessoa jurídica. Soma-se a isso, a implementação de um setor independente e com recursos capaz de assegurar o respeito ao programa, além de representar padrão de conduta dos próprios administradores. (FRAZÃO; OLIVA; ABILIO, 2019).

O c*omprometimento da alta administração* corresponde ao quarto elemento. Isso requer o comprometimento dos gestores com a incorporação e a observância de uma cultura empresarial que aplique e valorize as melhores práticas de gestão para atingir a *compliance*, pois:

> [...] caso a gerência da pessoa jurídica manifeste-se de forma contraditória com os planos constantes no programa de *compliance*, a mensagem recebida pelos funcionários será de que esse não passa de simples instrumento de fachada. (FRAZÃO; OLIVA; ABILIO, 2019, p. 690).

Corroborando tal entendimento, Janoni e Gieremek (2013) advertem que:

> [...] se os colaboradores de uma empresa perceberem que não há coerência entre as disposições do Código e as práticas adotadas na organização (por exemplo, sonegação de impostos, pagamentos realizados “por fora” do contrato de trabalho, condutas desrespeitosas aos direitos do trabalhador, maus-tratos), por mais bem feita que seja a norma, seguramente será tida como “letra morta”.

O quinto elemento relaciona-se à *autonomia e independência do setor de compliance*, o qual poderá ser um setor específico dentro da empresa ou então um escritório especializado para este fim. Independentemente da situação, o setor deve ser dotado de poderes para implementar políticas, procedimentos e controles

---

ali contidos, não será viável sua observância. Recomenda-se, ainda, que os documentos sejam de fácil e constante acesso, sem prejuízo de sua disponibilização periódica, ainda que não haja mudanças, e que se estruturem canais para dúvidas e esclarecimentos.” (FRAZÃO; OLIVA; ABILIO, 2019, p. 689).

[203] Soma-se a isso a edição da ISO 19600:2014, pela Organização Internacional de Normatização (*International Organization of Standardization* – ISO), a qual estabelece diretrizes para desenvolvimento, implantação, manutenção e avaliação do sistema de gestão de *compliance*. Trata-se de uma padronização, cuja adesão é voluntária, porém importante para a disseminação do *compliance*, “pois a tendência é que as empresas passem a exigir de seus fornecedores a certificação de implantação de normas estabelecidas na referida regra” (MATHIES, 2018, p. 141-142).

[204] Para maior aprofundamento sobre este ponto, remete-se o leitor ao item 3.4.

adequados, bem como ter capacidade para supervisionar e executar as normas previstas no programa, podendo tomar decisões sem a necessidade de recorrer a outras áreas.

O sexto elemento refere-se aos *treinamentos periódicos*, ou seja, as empresas devem promover treinamentos constantes e palestras explicativas tanto para os empregados quanto para os executivos, devendo ser consideradas as particularidades de cada setor e os riscos a que estão sujeitos, a fim de que todos compreendam o seu papel e contribuam para a minimização dos riscos. Para que isso aconteça:

> O *compliance* deve ser ativo, explicativo e acessível a todos, permitindo que as regras a serem seguidas sejam de conhecimento geral, que a respectiva execução seja acompanhada e que eventuais atos infratores possam ser identificados e/ou denunciados. (BLUM; ZAMPERLIN, 2016).

O sétimo elemento corresponde à *criação de uma cultura corporativa de respeito à ética e às leis*. Está relacionada à instituição de medidas preventivas, podendo ser utilizadas para combater condutas antiéticas e ilegais. No caso da LGPD, Pinheiro (2019) aponta que tal lei representou uma primeira etapa, sendo agora necessário um prazo para o mercado amadurecer e se adaptar às novas exigências. Além disso, a efetiva implementação da lei geral de proteção de dados "exige uma própria mudança de cultura, a fim de reconhecer que a titularidade e o controle dos dados pertencem aos respectivos titulares, de forma que as práticas empresariais deverão ser reestruturadas com esse propósito." (FRAZÃO; OLIVA; ABILIO, 2019, 2019, p. 691).

O *monitoramento constante dos controles e processos, inclusive para fins de atualização do programa* é enunciado como o oitavo elemento. A instituição do monitoramento permite identificar a existência de conflitos e possibilita a adoção de medidas corretivas. (MATHIES, 2018). De modo mais específico, "outra peculiaridade do *compliance* de dados é que certamente precisará de atualizações conforme evolua o estado das tecnologias utilizadas para a proteção de dados." (FRAZÃO; OLIVA; ABILIO, 2019, p. 692).

O penúltimo elemento refere-se à implementação de *canais seguros e abertos de comunicação de infrações e mecanismos de proteção dos informantes*. Tais canais auxiliam no saneamento de dúvidas, difundem comportamentos de

conformidade, facilitam o conhecimento de ilícitos pela empresa, permitem a adoção de medidas preventivas e impeditivas de novas condutas semelhantes, além de oportunizar a realização de denúncias. (FRAZÃO; OLIVA; ABILIO, 2019). Desse modo:

> [...] O empregado deve saber que tem a quem recorrer e que será ouvido, sem riscos de retaliação. Daí a necessidade de canais de denúncias, que admitam o anonimato, a fim de preservar a identidade daquele que, corajosamente, decidiu dividir a sua dor ou mesmo expor uma fragilidade sistêmica, de controles, ou um fato concreto. [...] Com essa medida, tanto se divulgará que a empresa não tolera malfeitos, sejam de que natureza for, como ouve os seus colaboradores e apura com rigor os fatos que sejam trazidos ao seu conhecimento. (JANONI; GIEREMEK, 2013).

Contudo, além da implementação dos canais, é importante instruir os funcionários para que evitem o seu emprego malicioso, sendo “salutar também estabelecer procedimentos a serem adotados no caso de recebimento de denúncia para identificar aquelas que não possuem plausibilidade.” (FRAZÃO; OLIVA; ABILIO, 2019, p. 693).

Por fim, a *detecção, apuração e punição de condutas contrárias ao programa de compliance* corresponde ao último elemento para identificar a sua robustez. Assim, “deve-se assegurar rápida e adequada punição às condutas a ele contrárias”, sob pena de a credibilidade do programa ser abalada e todo o trabalho perdido. (FRAZÃO; OLIVA; ABILIO, 2019, p. 693).

Vale destacar que, em se tratando de *compliance* de dados no âmbito laboral, não há um modelo único a ser seguido, porém, conforme exposto, a doutrina traça alguns elementos mínimos que, somado aos princípios previstos na LGPD, auxiliam na sua implementação. Ao lado destes, são apresentados três pilares, identificados como linhas mestras, responsáveis por dar a direção a ser adotada: prevenção, detecção e correção. (COMPLIANCE TOTAL, 2014).

O pilar de prevenção é considerado o mais importante, cabendo à instituição empregadora investir a maior parte de seus recursos para garantir a segurança das informações dos trabalhadores, evitando acessos não autorizados, bem como situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Em outras palavras, é preciso lembrar que em matéria de proteção de dados, é muito mais difícil recuperar um dado ou uma informação violados do que

defendê-los de uma primeira violação, especialmente se houver vazamento ou até mau uso dos dados sensíveis dos trabalhadores. (GOULART, 2014). Tal pilar se amolda ao poder diretivo de organização e direção do empregador.[205] (JOBIM, 2018). No sentido de se respeitar o princípio de prevenção, a doutrina fala:

> [...] no procedimento chamado de Privacy Impact Assessment (PIA), algo semelhante a um Estudo de Impacto Ambiental, porém direcionado às atividades tecnológicas. Assim, qualquer atividade que envolvesse a possibilidade de violação de privacidade, deveria ser precedida do PIA, a fim de se verificar os possíveis impactos. (GOULART, 2014, p. 80).

O segundo pilar relaciona-se à detecção, assumindo papel fundamental a existência de canais de denúncia como forma de controle eficaz dentro do ambiente laboral. (COMPLIANCE TOTAL, 2014). Este pilar pode ser desenvolvido por meio do poder diretivo fiscalizatório ou de controle do empregador. (JOBIM, 2018).

Já o pilar da correção refere-se à tolerância zero para desvios em relação aos valores e princípios éticos da instituição. Ocorrendo uma falha, esta deve ser corrigida de imediato, seguida da medida disciplinar pertinente, sob pena da credibilidade do programa ser abalada e todo o trabalho perdido. (COMPLIANCE TOTAL, 2014). Este pilar fortalece o poder diretivo disciplinar do empregador (JOBIM, 2018).

Vale destacar que o *compliance* em matéria de proteção de dados não é uma realidade apenas para as grandes companhias. A Lei nº 13.709/2018 aplica-se indistintamente a todas às pessoas natural ou jurídica de direito público ou privado, sem fazer distinção quanto ao porte[206]. Logo, implementar boas práticas para o tratamento dos dados pessoais dos trabalhadores e estar em conformidade com a legislação é uma exigência cada vez mais presente.

Nesse sentido, o próprio Conselho Administrativo de Defesa Econômica (CADE) “entende que pequenas e médias entidades podem implementar programas de *compliance*, ainda que eles sejam mais modestos e contem com orçamentos muito reduzidos em face dos programas de grandes companhias.” (CADE, 2016).

---

[205] Para maior aprofundamento sobre os poderes do empregador, remete-se o leitor ao item 2.2.

[206] Nesse sentido, verifica-se que o legislador esteve atento a tal questão, tanto que, ao tratar das “boas práticas e da governança”, estabeleceu, no artigo 50, § 2º, que a estrutura, a escala e o volume das operações deverão ser levados em conta, o que viabiliza a implementação de programa de *compliance* em matéria de dados independentemente do tamanho da empresa.

Portanto, ainda que estas empresas contem com quadro reduzido de trabalhadores, com menor fluxo de dados, guardadas as devidas proporções, elas podem implantar no âmbito laboral programas de *compliance*. Tal medida, se bem conduzida à luz dos elementos supramencionados, favorecerá o estabelecimento de uma cultura ética, pautada por normas e políticas internas que atendam às disposições da LGPD, evitando ou mitigando riscos reais e potenciais decorrentes do mau uso ou do uso abusivo dos dados aos direitos fundamentais do trabalhador.

Além dos elementos, dos princípios e dos pilares reportados, quando se fala em *compliance* de dados, surge outro aspecto de extrema importância: a *regulação pela tecnologia*. Embora a LGPD não se limite ao tratamento de dados no ciberespaço, é justamente neste cenário que ocorrem os maiores desafios.

Com efeito, como observa Bioni (2019, p. 05-06):

> [...] A informação é o (novo) elemento estruturante que (re)organiza a sociedade, tal como o fizeram a terra, as máquinas a vapor e a eletricidade, bem como os serviços, respectivamente, nas sociedade agrícola, industrial e pós-industrial.
> Ainda que essa nova forma de organização social não se resuma apenas ao meio ambiente virtual, a computação eletrônica e a Internet são as ferramentas de destaque desse processo.

Disso decorre:

> [...] a necessidade de que os programas de *compliance* de dados não se limitem apenas à previsão de princípios ou regras de comportamento, mas visem também à adoção de tecnologias que possam ser compatíveis com a eficácia de tais regras. (FRAZÃO; OLIVA; ABILIO, 2019, p. 710).

Com relação ao ciberespaço e a circulação de dados, ressalta-se que umas das grandes preocupações consiste em como proteger os dados dos trabalhadores na chamada economia colaborativa. Como salientado no segundo capítulo, as relações de trabalho vêm passando por uma reconfiguração em âmbito mundial, sendo cada vez mais comum novas e emergentes formas de trabalho, especialmente aquelas por meio de aplicativos digitais.

Tamanha a relevância do tema que, na 108ª Conferência Internacional do Trabalho, que marcou a celebração do Centenário da OIT, foi promulgada a Declaração do Centenário, a qual coloca o ser humano como o centro das políticas laborais e reconhece a necessidade de que se estabeleça um piso mínimo de direitos independente da natureza do vínculo de emprego existente. O texto, além de reafirmar

os princípios da Declaração da Filadélfia, assegura a todos os trabalhadores, independentemente do seu *status*, a garantia da proteção da privacidade e dos dados pessoais.[207] (OIT, 2019).

Assim, frente ao atual contexto[208], os diretos fundamentais inespecíficos (em especial a privacidade, a proteção de dados e a reserva da intimidade) dos trabalhadores de plataformas estão cada vez mais ameaçados.

Os gigantes dos aplicativos exercem um controle cada vez mais instrusivo e perigoso, feito à distância pelos algoritmos e pela inteligência artificial, que recolhem as pistas digitais deixadas (in)voluntariamente pela rede mundial de computadores. Em conjunto, tais "pistas" conferem um poder de controle da informação, permitindo aos seus detentores a realização de operações com os dados pessoais daqueles que lhe prestam serviço, bem como a criação de perfis. Disso decorre a necessidade de proteção dos dados pessoais e sensíveis destes trabalhadores digitais.

Sobre o tema, o Conselho da União Europeia aprovou em abril de 2019 o regulamento relativo à promoção da equidade e da transparência para os utilizadores profissionais de serviços de intermediação em linha. Trata-se um regulamento inédito, cujo objetivo é introduzir novas regras que proporcionem às empresas um enquadramento mais transparente, justo e previsível, e que tenha vias de recurso rápidas e eficientes. (CONSELHO EUROPEU, 2019).

No que tange aos dados, incluindo os dados pessoais, o regulamento estabelece que cabe aos prestadores de serviços de intermediação em linha transmitir aos utilizadores profissionais uma descrição clara do âmbito de aplicação, da natureza e das condições de acesso e utilização de determinadas categorias de dados.[209]

---

[207] Item III, "B", "v", da Declaração do Centenário da OIT.

[208] Com relação ao contexto, o Conselho Europeu aponta que "As plataformas em linha são facilitadores fundamentais do comércio digital. Atualmente, mais de um milhão de empresas da UE fazem negócio através de plataformas em linha, a fim de alcançarem os seus clientes, e estima-se que cerca de 60 % do consumo privado e 30 % do consumo público de bens e serviços relacionados com o total da economia digital sejam efetuados por recurso a intermediários em linha. Apesar de oferecerem um grande potencial em termos de acesso eficiente aos mercados (transfronteiras), as empresas europeias não conseguem atualmente explorar todo o potencial da economia das plataformas em linha devido a várias práticas comerciais potencialmente prejudiciais e à falta de mecanismos de recurso eficazes na UE. Ao mesmo tempo, os prestadores de serviços em linha enfrentam dificuldades quando operam no mercado único devido à emergente fragmentação do mesmo." (CONSELHO EUROPEU, 2019).

[209] De acordo com o considerando 34 do regulamento, "[...] é importante que os utilizadores profissionais tenham conhecimento se o prestador de serviços partilha com terceiros alguns dados que tenham sido gerados pela utilização do serviço de intermediação por parte do utilizador profissional. Em especial, os utilizadores profissionais deverão ser informados de toda a partilha de dados com terceiros que ocorra para fins não necessários ao bom funcionamento dos serviços de intermediação em linha; por exemplo, caso o fornecedor utilize esses dados para fins lucrativos. Para que os

Nesse sentido, importante destacar que a parte final do consdierando 35 do regulamento prevê expressamente que:

> O tratamento dos dados pessoais deverá respeitar o regime jurídico da União relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais, ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas, mais particularmente o Regulamento (UE) 2016/6791, a Diretiva (UE) 2016/6802 e a Diretiva 2002/58/CE3 do Parlamento Europeu e do Conselho. (UNIÃO EUROPEIA, 2019, p. 30).

O regulamento também estabelece obrigações de transparência para as plataformas digitais, obrigando estas a utilizarem termos e condições claros e inteligíveis para a prestação dos seus serviços de intermediação em linhas, fornecendo uma exposição de motivos quando decidirem suspender, restringir ou pôr termo à utilização dos seus serviços por um utilizador profissional. Soma-se a isso a necessidade de as plataformas divulgarem publicamente os principais parâmetros que determinam a classificação dos utilizadores nos resultados de pesquisa. (CONSELHO EUROPEU, 2019).

Como visto no capítulo 02, com o fenômeno da “uberização” do trabalho, as decisões da empresa proprietária da plataforma, inclusive o próprio desligamento daqueles trabalhadores que atuam nas plataformas, passou a ser realizado mediante avaliações de terceiros (usuários-clientes), que atribuem pontos, estrelas ou outros símbolos para classificar o serviço prestado.

Contudo, com a aprovação do regulamento, ainda que restrito à União Europeia, trata-se de um primeiro passo para que as plataformas digitais divulguem os motivos porque estão suspendendo, por exemplo, um motorista de *uber*, ou, ainda, os principais parâmetros utilizados nos *hankings* para a seleção de prestadores de serviços.

Além disso, o regulamento também obriga todas as plataformas (exceto as pequenas[210]) a criarem um sistema interno de tratamento de reclamações rápido e eficiente e a apresentarem anualmente um relatório sobre a sua eficácia.

---

utilizadores profissionais possam exercer plenamente os seus direitos de influenciar esta partilha de dados, os prestadores de serviços de intermediação em linha deverão também ser explícitos relativamente a eventuais faculdades de autoexclusão da partilha de dados previstas na sua relação contratual com o utilizador profissional.” (UNIÃO EUROPERIA, 2019).

[210] De acordo com o considerando 38 do Regulamento, tendo em conta os custos, os prestadores de serviços de intermediação em linha que sejam pequenas empresas (em conformidade com as disposições da Recomendação 2003/361/CE da Comissão, de 6 de maio de 2003, relativa à definição

Com efeito, revela-se de extrema importância a criação de um sistema que lide rapidamente com as queixas, isso porque, assim como os demais trabalhadores, os profissionais que prestam serviços por meio destas platafomas, também estão sujeitos a avaliações, a sanções disciplinares, a práticas de assédio, aos riscos à saúde (em razão do *stress*, das longas jornadas, dentre outros fatores)[211], sem que houvesse até o presente momento a possiblidade de reclamação.

O regulamento também exige que as plataformas incluam, nos seus termos e condições, dois ou mais mediadores para os casos em que o sistema interno de tratamento de reclamações não permita resolver um litígio entre utilizadores empresariais. Além disso, estabelece o direito das organizações e associações representativas ou dos organismos públicos a iniciarem um processo judicial contra plataformas que não cumpram os requisitos do regulamento, sendo autorizado os Estados-Membros definirem sanções conformes com os seus sistemas nacionais em caso de infração. (CONSELHO EUROPEU, 2019).

Logo, dada a peculiaridade das plataformas digitais, as quais contam com milhões de utilizadores profissionais e com atuação em âmbito mundial, tem-se que o regulamento da União Europeia, embora destinado às plataformas estabelecidas na UE e que ofereçam bens ou serviços a consumidores que também estejam localizados na UE, traça elementos característicos de um programa de *compliance*, inclusive com diretrizes que podem ser estendidas para a proteção dos dados.

Conforme se verifica, o regulamento prevê a elaboração de códigos de conduta por parte dos prestadores de serviços de intermediação em linha e das organizações e associações que os representem, juntamente com os utilizadores profissionais. Também estabelece que devem ser levadas em consideração as características específicas dos setores em causa. Além disso, os prestadores de serviços de intermediação devem disponibilizar facilmente as informações relativas ao funcionamento e à eficácia dos seus procedimentos internos de tratamento de reclamações, os quais são passíveis de atualização periódica. Ou seja, ainda que com outras palavras, o regulamento traça elementos característicos de um programa de comprometimento para as empresas proprietárias de plataformas digitais.

---

de micro, pequenas e médias empresas), estão isentos da obrigação de implementar procedimentos internos de tratamento de reclamações. Contudo, nada impede que estas empresas venham a estabelecer de forma voluntária tais procedimentos, devendo, no caso, observar os critérios definidos no regulamento. (UNIÃO EUROPEIA, 2019).

[211] Para maior aprofundamento, remete-se o leitor ao item 2.4.

No caso, quando estas empresas realizam o tratamento dos dados pessoais e sensíveis dos utilizadores profissionais, elas também se tornam responsáveis pela segurança destes dados, sendo a implementação do *compliance* de dados uma forma eficaz de protegê-los.

Nesse sentido, como estas empresas atuam sobretudo em meio digital, a tecnologia também pode ser utilizada como um importante instrumento para a promoção dos programas de integridade de dados. Nesse sentido:

> Se por um lado, a tecnologia pode ser invasiva à privacidade informacional, [...] Por outro lado, ela pode ser uma ferramenta para a proteção dos dados pessoais, tal como propõem as denominadas *Privacy Enhancing Technologies*/PETs[212]. (BIONI, 2019, p. 176).

Assim, seja para as típicas relações de trabalho, seja para as novas configurações, em ambas a desigualdade entre as partes é manifesta. Logo, as PETs apresentam-se como uma possível solução para a equalização das assimetrias do mercado informacional, a fim de que o cidadão-trabalhador, titular dos dados, diante da sua (hiper)vulnerabilidade, possa ser empoderado com um melhor controle sobre os seus dados. (BIONI, 2019).

Por fim, após examinada a nova cultura de *compliance* e sua incidência no âmbito laboral para a proteção dos dados pessoais e sensíveis dos trabalhadores, o tópico seguinte versará sobre a responsabilidade do empregador quanto ao tratamento destes dados.

4.3 A RESPONSABILIDADE DO EMPREGADOR NO TRATAMENTO DOS DADOS PESSOAIS

No contexto laboral, o tratamento dos dados pessoais e sensíveis tem um impacto substancial, uma vez que qualquer empresa que tenha trabalhadores a seu cargo, ainda que seja de pequeno ou médio porte, ou uma empresa vocacionada para

---

[212] Segundo a tradução literal – PETs correspondem a "tecnologias que reforçam-melhoram a privacidade – denota abrangência do termo que, como um *guarda-chuva*, é capaz de abarcar toda e qualquer tecnologia que seja amigável e facilitadora à privacidade." Como exemplo dessas tecnologias, menciona-se "a criptografia que assegura a confidencialidade das comunicações. Ou, ainda, a anonimização dos dados pessoais que quebra ou pelo menos dificulta o vínculo de identificação entre um dado e o sujeito ao qual ele está atrelado [...], bem como mecanismos de navegação anônima que impedem o rastreamento do usuário." (BIONI, 2019, p. 176-177).

o recrutamento ou trabalho temporário ou mesmo os grandes grupos empresariais, todos estão obrigados a estar em conformidade com as exigências estabelecidas pela LGPD.

Como mencionado, no decorrer das relações de trabalho, o empregador ou aqueles que agem em seu nome, entram em contato com inúmeros dados e informações que revelam aspectos da vida privada dos trabalhadores, tais como dados acadêmicos, profissionais, hábitos de vida, assim como questões relacionadas a aspectos ideológicos, políticos, religiosos, entre outros, isso porque:

> [...] O empregador precisa de determinados dados pessoais para a assinatura do contrato e precisa tê-los em mãos para muitas das operações que devem ser realizadas no tráfego regular da empresa (recibo de salários, retenções fiscais, contribuições para a seguridade social, descontos para uma ou outra razão, etc.). Tudo isso requer a coleta de informações e, normalmente, o processamento dos dados (por meio de um arquivo ou instrumento similar). Como vimos, as regras em matéria de proteção de dados pessoais permitem o conhecimento e o tratamento dos dados necessários para o funcionamento da relação de trabalho, mas, ao mesmo tempo, impõem algumas exigências ao empregador, que terá que enfrentar novas obrigações e novas responsabilidades.[213] (MURCIA; CARDO, 2019, p. 11-12, tradução nossa).

A LGPD é uma norma com alcance geral e obrigatória em todos os seus aspectos. Embora não se destine, precipuamente, às relações de trabalho, atinge as relações jurídicas que envolvam manuseio de dados ou informações, tendo por objetivo principal proteger os direitos fundamentais de liberdade e de privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural.

Logo, apesar de não mencionar as relações laborais, evidente que estas e outras relações conexas, que envolvam a prestação de serviços em geral, compreendem, também, um fluxo de informações ou dados. Desse modo, inegável que o ambiente de trabalho configura campo fértil para o tratamento de dados pessoais e sensíveis, na medida em que estes são amplamente obtidos, usados, armazenados e divulgados, tornando os agentes de tratamento implicados nesta

---

[213] *[...] el empleador necesita determinados datos personales para la firma del contrato y necesita tener a mano esos datos para muchas de las operaciones que debe llevar a cabo en el tráfico ordinario de la empresa (recibo de salarios, retenciones fiscales, cotizaciones a la seguridad social, descuentos por uno u otro concepto, etc.). Para todo ello se requiere el acopio de información y, normalmente, el procesamiento de los datos (mediante un fichero o instrumento similar). Como hemos visto, las normas sobre protección de datos personales permiten el conocimiento y tratamiento de los datos necesarios para el funcionamiento de la relación laboral, pero imponen al mismo tiempo algunas exigencias al empresario, que tendrá que hacer frente a nuevos deberes y nuevas responsabilidades*.

relação responsáveis pela observância e cumprimento das normas de proteção de dados.

Assim, a nova normativa estabelece obrigações direcionadas aos agentes responsáveis pelo tratamento dos dados, cuja conduta deve pautar-se pelo princípio de responsabilidade e prestação de contas, também conhecida pelo termo *accountability*. [214]

Nesse contexto, a Lei nº 13.709/2018 consagra o aludido princípio no artigo 6º, inciso X, ao prever expressamente que o agente deve demonstrar a "adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas." (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

Diante disso, a introdução do princípio em questão assume:

> [...] um papel fundamental como instrumento de compliance, ao promover a implementação, por parte do responsável pelo tratamento, das garantias necessárias ao cumprimento das regras de proteção de dados e respetiva demonstração, tanto a nível interno como externo. (LOPES, 2018, p. 55).

Em igual sentido, o *compliance* de dados pessoais auxilia os agentes de tratamento a aplicar de forma eficaz as normas de proteção de dados, na medida em que conduz "a pessoa jurídica a manter esses dados e toda sua atividade dentro dos ditames legais, utilizando a segurança da informação em prol da minimização de incidentes que impliquem na responsabilidade empresarial." (BLUM; ZAMPERLIN, 2016).

Partindo disso, antes de entrar no tema da responsabilidade pelo tratamento dos dados no âmbito das relações laborais, importante analisar quem são os sujeitos envolvidos nesta relação e qual a posição ocupada por cada um à luz da LGPD.

De acordo com a Lei nº 13.709/2018, a figura do titular corresponde à "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento"

---

[214] O princípio da responsabilidade "foi pela primeira vez introduzido no contexto da proteção de dados, a nível internacional, nas *Guidelines* da OCDE, adotadas em 23 de setembro de 1980. A partir dessa data, a sua importância tem vindo a ser discutida em inúmeros fóruns internacionais dedicados à matéria de proteção de dados. Em especial, destaca-se a *Opinion 3/2010 on the principle of accountability*, emitida pelo 'Grupo de proteção das pessoas no que diz respeito ao tratamento de dados pessoais' contemplado no artigo 29.º da Diretiva 95/46/CE (G29)20, na qual foi defendida a introdução deste princípio na revisão do regime geral de proteção de dados, com o objetivo de reafirmar e reforçar a responsabilidade do responsável pelo tratamento." (LOPES, 2018, p. 52-53).

(artigo 5º, V). O controlador e o operador são agentes de tratamento (artigo 5º, IX), sendo o controlador definido como a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" (artigo 5º, VI) e, o operador, a "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (artigo 5º, VII).[215]

Em face dos conceitos apresentados e, à luz da relação de emprego, nos termos dos artigos 2º e 3º da CLT, o empregado (ou o trabalhador numa concepção mais ampla) corresponde à figura do *titular dos dados*, o qual, por força do contrato de trabalho, fornece informações ao empregador. Este, por sua vez, será o *controlador* desses dados, competindo-lhe tomar as decisões necessárias sobre o tratamento a ser realizado por um *operador*, posição que pode ser do próprio empregador, de um preposto, de um setor da empresa, ou de um terceiro, externo à relação laboral.

Assim, o empregador, na posição de controlador, toma as decisões referentes às finalidades e aos meios de tratamento dos dados pessoais e sensíveis dos trabalhadores. Contudo, há situações em que este tratamento é delegado. Para tais circunstâncias, a OIT, no item 5.9 do Repertório de Recomendações Práticas em matéria de proteção de dados, chama a atenção para a necessidade de uma formação periódica das pessoas que farão o tratamento, nos seguintes termos:

> As pessoas encarregadas pelo tratamento de dados pessoais devem receber periodicamente uma formação que lhes permita compreender o processo de coleta dados e seu papel na aplicação dos princípios estabelecidos no presente Repertório.[216] (OIT, 1997, p. 02, tradução nossa).

Além disso, acerca do acesso aos dados pessoais, o item 10.6 do Repertório dispõe que "dentro da empresa, os dados pessoais somente devem ser colocados à disposição de usuários especificamente autorizados, que só tenham

---

[215] A LGPD, ao tratar do controlador e do colaborador, estabelece no artigo 37 que eles "devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse." Além disso, o artigo 39 determina 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." (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

[216] [...] *Las personas encargadas del tratamiento de datos personales deberían recibir periódicamente una formación que les permita comprender el proceso de acopio de datos y el papel que les corresponde en la aplicación de los principios enunciados en el presente repertorio*.

acesso àqueles necessários para o cumprimento de suas tarefas específicas."[217] (OIT, 1997, p. 06, tradução nossa).

A distinção dos atores envolvidos na atividade de tratamento dos dados é extremamente relevante para fins de responsabilização, pois, a depender da posição ocupada pelo agente (se controlador ou operador), bem como das ações por ele praticadas (se envolve processo decisório ou tão somente agir de acordo com as instruções recebidas), será fixada a responsabilidade de cada um dos envolvidos. Contudo:

> [...] devido à crescente complexidade das operações de tratamento de dados, tais como os dados tratados em *cloud*, redes sociais, motores de busca, em que nem sempre é claro para o titular dos dados quem determina se e como os dados são tratados e, portanto, a quem deve ser alocada a responsabilidade. Tal incerteza é suscetível de provocar efeitos negativos no cumprimento das regras de proteção de dados e na eficácia da legislação de proteção de dados como um todo. (LOPES, 2018, p. 58).

Disso decorre a importância de se definir de forma clara os conceitos de controlador e operador, conferindo orientações para aplicar a sua distinção de forma objetiva a fim de apurar a responsabilidade de cada um.

Em termos de responsabilização, no Brasil, o Código Civil dispõe no artigo 186[218], combinado com o artigo 927[219], sobre o instituto da responsabilidade civil. A Consolidação das Leis do Trabalho (CLT), por seu turno, disciplina a reparação civil por danos extrapatrimoniais nos artigos 223-A a 223-G. Porém, em matéria de proteção de dados pessoais, o legislador optou por dispor sobre o assunto entre os artigos 42 a 45. Assim, antes de examinar a responsabilidade à luz da Lei nº 13.709/2018, convém traçar, ainda que brevemente, o que se entende por responsabilidade civil.

Nessa perspectiva, segundo a doutrina:

> [...] a noção jurídica de responsabilidade pressupõe a atividade danosa de alguém que, atuando *a priori* ilicitamente, viola uma norma jurídica

---

[217] [...] *En el seno de la empresa, los datos personales sólo deberían ponerse a la disposición de usuarios específicamente autorizados, que únicamente tengan acceso a los que precisen para el cumplimiento de sus tareas concretas*.

[218] "Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito." (BRASIL. Lei nº 10.406, de 10 de janeiro de 2002).

[219] "Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo." (BRASIL. Lei nº 10.406, de 10 de janeiro de 2002).

> preexistente (legal ou contratual), subordinando-se, dessa forma, às consequências do seu ato (obrigação de reparar). (GAGLIANO; PAMPLONA FILHO, 2017, p. 858).

Nesse sentido:

> [...] o foco atual da responsabilidade civil, pelo que se percebe da sua evolução histórica e tendências doutrinárias, reside cada vez mais no imperativo de indenizar ou compensar dano injustamente sofrido, abandonando-se a preocupação com a censura do seu responsável. (FACCHINI NETO, 2010, p. 26).

Portanto, pode-se afirmar que responsabilidade exprime a ideia de reparação do dano causado, de "restauração do equilíbrio rompido". (BITTAR, 2015, p. 20). Dentro dessa visão, uma das tendências modernas consiste justamente em ampliar a abrangência da teoria da responsabilidade civil, a fim de possibilitar que todo e qualquer dano possa ser reparado. (FACCHINI NETO, 2010).

Dando sequência, a doutrina aponta que embora a função originária e primordial da responsabilidade civil seja a função reparatória (de danos materiais) ou compensatória (de danos extrapatrimoniais), outras funções podem ser desenhadas pelo instituto, hipótese em que "avultam as chamadas funções punitiva[220] e dissuasória[221]", tal como aponta Facchini Neto (2010, p. 27).

Ainda no tema da responsabilidade civil, o Direito brasileiro, basicamente, conta com duas categorias: a subjetiva e a objetiva. A primeira é a decorrente de dano causado em função de ato doloso ou culposo. Esta culpa se caracteriza quando o agente causador do dano atuar com negligência, imprudência ou imperícia. A noção

---

[220] Facchini Neto (2010, p. 28-29) explica que, após a definitiva demarcação dos espaços destinados à responsabilidade civil e à responsabilidade penal, a função punitiva ficou confinada a esta última. Todavia, ao se aceitar a compensabilidade dos danos extrapatrimoniais, percebeu-se que ali também estava presente a ideia de uma função punitiva da responsabilidade civil. Como exemplo, menciona o caso dos familiares da vítima de um homicídio: "a obtenção de uma compensação econômica paga pelo causador da morte representa uma forma estilizada e civilizada de vingança, pois no imaginário popular está-se também a punir o ofensor pelo mal causado quando ele vem a ser condenado a pagar uma indenização." Além disso, aponta que "com a enorme difusão contemporânea da tutela jurídica (inclusive através de mecanismos da responsabilidade civil) dos direitos da personalidade, recuperou-se a ideia de *penas privadas*. Daí um certo *revival* da função punitiva, tendo sido precursores os sistemas jurídicos integrantes da família da *common law*, através dos conhecidos *punitive* (ou *exemplary*) *dammages*.

[221] A função dissuasória busca dissuadir condutas futuras, ou seja, "através do mecanismo da responsabilização civil, busca-se sinalizar a todos os cidadãos sobre quais condutas a evitar, por serem reprováveis do ponto de vista ético-jurídico. [...] Na responsabilidade civil com função dissuasória, porém, o objetivo de prevenção geral, de dissuasão ou de orientação sobre condutas a adotar, passa a ser o escopo principal. O meio para alcançá-lo, porém, consiste na condenação do responsável à reparação/compensação de danos individuais. (FACCHINI NETO, 2010, p. 28-29).

básica da responsabilidade civil, dentro da doutrina subjetiva, é o princípio segundo o qual cada um responde pela própria culpa. (GAGLIANO; PAMPLONA FILHO, 2017).

No entanto, "há situações em que o ordenamento jurídico atribui a responsabilidade civil a alguém por dano que não foi causado diretamente por ele, mas sim por um terceiro com quem mantém algum tipo de relação jurídica."[222] Trata-se de uma "responsabilidade civil indireta, em que o elemento culpa não é desprezado, mas sim presumido, em função do dever geral de vigilância a que está obrigado o réu." (GAGLIANO; PAMPLONA FILHO, 2017, p. 862).

Entretanto, existem hipóteses nas quais não é necessário sequer ser caracterizada a culpa. Tais casos correspondem ao que se convencionou chamar de responsabilidade civil objetiva, na qual o dolo ou culpa na conduta do agente causador do dano é irrelevante, sendo somente necessária a existência do elo de causalidade entre o dano e a conduta do agente responsável, para que surja o dever de indenizar. (GAGLIANO; PAMPLONA FILHO, 2017).

A LGPD adota critérios específicos para a responsabilidade e o dever de indenizar. Assim, no que tange à responsabilização, o artigo 42 da LGPD dispõe que, se a conduta do agente causar dano a outrem, haverá a obrigação de reparar:[223]

---

[222] A título exemplificativo, menciona-se o inciso III do artigo 932 do Código Civil, que dispõe: "Art. 932. São também responsáveis pela reparação civil: [...] III – o empregador ou comitente, por seus empregados, serviçais e prepostos, no exercício do trabalho que lhes competir, ou em razão dele;" (BRASIL. Lei nº 10.406, de 10 de janeiro de 2002).

[223] Sobre o tema da responsabilidade na LGPD, há divergência quanto a sua espécie: se objetiva ou subjetiva, o que se percebe a partir da leitura do Parecer ao Projeto de Lei nº 4.060/2012 (que deu origem à Lei Ordinária nº 13.709/2018). Segundo os debates da Comissão Especial, "a responsabilidade civil possui diferentes tratamentos de acordo com cada país. A União Europeia, por exemplo, determina que haja responsabilidade do Responsável independente de culpa, mas não do Operador, que só responderá na hipótese em que transgredir obrigações específicas a ele direcionadas ou agir contrariamente às instruções legítimas do Responsável. A legislação brasileira adota a regra geral de responsabilidade objetiva, aquela que independe de culpa do infrator, quando há relação de consumo (conforme o Código de Defesa do Consumidor, arts. 7º e 12). E também há responsabilidade objetiva quando a atividade desenvolvida é considerada de risco, como podem ser consideradas as atividades relacionadas ao tratamento de dados pessoais (conforme o Código Civil, parágrafo único do art. 927). Cabe perquirir se esse tratamento é o mais adequado ou se haveria exceções possíveis a ensejar reponsabilidade subjetiva em alguma parte da cadeia de valor que congrega as atividades de tratamento de dados pessoais." Avançando nas discussões, Audiência Pública realizada 03/05/17 focou no tema "Responsabilidade Objetiva e Solidária". "Rafael Zanatta representando o IDEC (Instituto Brasileiro de Defesa do Consumidor) salientou a hipossuficiência do usuário na atividade de risco que representa a coleta de dados. Defendeu a responsabilidade objetiva e solidária, conforme o caso. Leonardo Bessa, diretor do BRASILCON (Instituto Brasileiro de Política e Direito do Consumidor) também defendeu esse tipo de responsabilidade e salientou que o Código Civil, arts. 159 e 927, garante que atividades que impliquem em risco devem ser enquadradas como de responsabilidade objetiva. Sugeriu, também, incluir no art. 42 do PL a expressão "independente de culpa". Por fim, Leandro Alvarenga da CNDL (Confederação Nacional de Dirigentes Lojistas) defendeu que a responsabilidade do agente de tratamento deveria ser subjetiva e não envolver toda a cadeia, sob pena de engessar a

> O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

Da leitura do dispositivo, verifica-se que o dano deve ocorrer em função da atividade de tratamento de dados pessoais, podendo ser um dano imaterial ou extrapatrimonial, do qual o dano moral, assim como o existencial e o temporal, são espécies, podendo também ser de ordem individual ou coletiva, e deve ocorrer em violação à legislação de proteção de dados pessoais.

Além disso, o parágrafo primeiro do artigo 42 da LGPD estabelece uma garantia de efetiva indenização, ou seja, uma espécie de compensação ao titular dos dados, a fim de que o exercício de seu direito não seja prejudicado, tal como ocorre no âmbito do Direito do Consumidor[224] e na seara trabalhista[225]:

> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
> I – o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
> II – os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei. (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).[226]

Verifica-se que o inciso I prevê uma relação de solidariedade entre os agentes pelos danos causados pelo tratamento, seja porque o operador descumpriu

---

economia e prejudicar, principalmente, os pequenos empresários." (CÂMARA DOS DEPUTADOS, 2018, p. 12, 17 e 18).

[224] Nesse sentido, o artigo 25, parágrafo primeiro, dispõe que "havendo mais de um responsável pela causação do dano, todos responderão solidariamente pela reparação prevista nesta e nas seções anteriores." (BRASIL. Lei 8.078, de 11 de setembro de 1990).

[225] Com relação ao tema, o artigo 2º, parágrafo segundo prevê que: [...] "Sempre que uma ou mais empresas, tendo, embora, cada uma delas, personalidade jurídica própria, estiverem sob a direção, controle ou administração de outra, ou ainda quando, mesmo guardando cada uma sua autonomia, integrem grupo econômico, serão responsáveis solidariamente pelas obrigações decorrentes da relação de emprego." (BRASIL. Decreto-Lei nº 5.452, de 1º de maio de 1943).

[226] Com relação ao dispositivo, o Parecer ao Projeto de Lei nº 4.060/2012 menciona que "Tendo ainda em vista que o tratamento de dados frequentemente envolve mais de um agente e como não deve ser do titular dos dados o ônus de descobrir dentro de uma cadeia econômica quem deu causa ao dano sofrido, o **§ 1° do art. 42** estipula a **responsabilidade solidária sempre que houver responsáveis atuando em conjunto,** bem como estabelece a responsabilidade solidária do operador quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do responsável." (CÂMARA DOS DEPUTADOS, 2018, p. 41).

as obrigações legais de proteção de dados, seja porque não observou as instruções lícitas do controlador, hipótese em que será equiparado ao controlador para fins de responsabilização.

Portanto, ocorrendo tais situações, a LGPD estabelece a possibilidade de múltiplos corresponsáveis pelo tratamento, com iguais ou diferentes graus de responsabilidade, o que não impede que o titular dos dados exerça o seu direito de ação contra qualquer um dos agentes ou contra todos os responsáveis pelo tratamento. Tanto é assim que o § 4º do artigo 42 da LGPD assegura que "aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso." (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

O inciso II do § 1º do artigo 42 também prevê uma garantia solidária, ao estabelecer que se se houver mais de um controlador diretamente envolvido no tratamento dos dados, todos responderão solidariamente, podendo o titular dos dados propor ação em face de qualquer um dos controladores pelo total da indenização, assegurado àquele que reparar o dano o direito de regresso contra os demais envolvidos, tal como previsto no inciso I.

O artigo 43 da LGPD, por sua vez, elenca três hipóteses em que os agentes de tratamento não serão responsabilizados.[227] Para tanto, cabe aos agentes provar que: a) não realizaram o tratamento de dados pessoais que lhes foi atribuído; b) se realizaram o tratamento, não houve violação à legislação de proteção de dados; ou c) o dano é decorrente de culpa exclusiva do titular de dados ou de terceiro. A segunda hipótese configura um incentivo à adoção da LGPD, na medida em que, havendo total aderência aos seus comandos, a responsabilidade civil ficará excluída.

Além disso, o § 2º do artigo 42 da LGPD assegura a garantia processual de inversão do ônus da prova.[228] Trata-se da hipótese em que o juiz poderá inverter

---

[227] O artigo 43 da LGPD, tal como o artigo 12, § 3º, do Código de Defesa do Consumidor, prevê hipóteses de exceção à responsabilidade civil do responsável e do operador.

[228] Sobre tal questão, o Parecer ao Projeto de Lei nº 4.060/2012 defende "a incidência da teoria dinâmica do ônus da prova, segundo a qual tal ônus deve recair sobre a parte que tiver maiores condições de dele se desincumbir, à vista da cooperação e da boa-fé processual. (CÂMARA DOS DEPUTADOS, 2018, p. 41). Tal garantia encontra-se prevista no CDC, no inciso VIII do artigo 6º, o qual estabelece dentre os direitos básicos do consumidor, "a facilitação da defesa de seus direitos, inclusive com a inversão do ônus da prova, a seu favor, no processo civil, quando, a critério do juiz, for verossímil a alegação ou quando for ele hipossuficiente, segundo as regras ordinárias de experiências." (BRASIL. Lei 8.078, de 11 de setembro de 1990). O novo Código de Processo Civil também prevê tal inversão no artigo 373, § 1º, nos seguintes termos: "Nos casos previstos em lei ou diante de peculiaridades da causa relacionadas à impossibilidade ou à excessiva dificuldade de cumprir o encargo nos termos

tal ônus se: a) a alegação do titular for verossímil; b) houver hipossuficiência para fins de produção de prova; ou c) quando a produção da prova for excessivamente onerosa ao titular.

O § 3º do artigo 42 da LGPD autoriza o ajuizamento de ações de reparação por danos coletivos que tenham por objeto a responsabilização dos agentes que, em razão do exercício de atividade de tratamento de dados pessoais, tenham causados danos aos seus titulares.

Quanto às relações laborais, no caso de haver ameaça ou violação aos dados pessoais e sensíveis dos trabalhadores, tanto o sindicato (artigo 8º, inciso III, da CF), quanto o órgão ministerial do trabalho (artigo 129, § 1º, da CF) têm legitimidade para atuar na garantia ou no reestabelecimento da proteção a este direito fundamental dos trabalhadores.

Com relação às hipóteses de irregularidade, o artigo 44 da LGPD estabelece que o tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as seguintes circunstâncias, dentre outras: a) o modo pelo qual o tratamento é realizado; b) o resultado e os riscos que razoavelmente dele se esperam; e c) as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Já o parágrafo único do artigo 44 da LGPD apresenta mais uma hipótese de dano a ser indenizado. Trata-se dos danos decorrentes da violação de segurança dos dados, quando os agentes deixarem de adotar as medidas previstas no artigo 46.[229]

Por fim, o artigo 45 da LGPD estabelece que “as hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.” (BRASIL, Lei nº 13.709, de 14 de agosto de 2018). Ou seja, o dispositivo atendeu à preocupação de que a regra de responsabilidade do CDC, aplicável aos vícios ou defeitos no fornecimento de bens

---

do caput ou à maior facilidade de obtenção da prova do fato contrário, poderá o juiz atribuir o ônus da prova de modo diverso, desde que o faça por decisão fundamentada, caso em que deverá dar à parte a oportunidade de se desincumbir do ônus que lhe foi atribuído.” (BRASIL. Lei 13.105, de 16 de março de 2015).

[229] A Lei nº 13.709/2018, em complemento ao princípio da responsabilidade, previu um conjunto de medidas técnicas e organizativas a fim de assegurar e demonstrar, por parte do responsável pelo tratamento, o cumprimento das regras de proteção de dados. O estudo desse conjunto de medidas será objeto do item 4.4.

ou serviços, não fossem revogados pela LGPD. Consequentemente, os aspectos de consumo (como os vícios ou defeitos de um produto, por exemplo) permanecem submetidos à regra de responsabilidade objetiva e solidária do CDC.

No caso dos dados pessoais e sensíveis dos trabalhadores, diferentemente do que ocorre com as relações de consumo, a LGPD foi silente quanto à responsabilidade civil do empregador pelos danos causados aos titulares dos dados (trabalhadores).

Apesar disso, como mencionado, a CLT disciplina a reparação civil por danos extrapatrimoniais nos artigos 223-A a 223-G, sendo que, de acordo com Goldschmidt (2019a, p. 131) o artigo 223-A da CLT "inaugura um microssistema de responsabilidade civil por danos extrapatrimoniais no âmbito das relações de trabalho."

Nesse sentido, como indicado no terceiro capítulo, o artigo 223-C da CLT prevê um rol aberto de bens extrapatrimoniais juridicamente tuteláveis, a partir do qual é possível extrair a proteção aos dados pessoais e sensíveis dos trabalhadores.[230]

Diante disso, frente à especialidade[231] e, somado ao fato de que, no cotejo da LGPD com a CLT, há de se aplicar a norma mais benéfica ao trabalhador[232], entende-se aplicável o novel regime dos artigos 223-A a 223-G da CLT às situações nas quais o empregador causar danos em razão do exercício de atividade de tratamento de dados pessoais e sensíveis dos trabalhadores.

Além da responsabilidade civil, a LGPD também estabelece sanções administrativas em caso de descumprimento das normas previstas em matéria de proteção de dados, cuja aplicação fica a cargo da Autoridade Nacional de Proteção de Dados (ANPD)[233].

---

[230] Para maior aprofundamento do tema, remete-se o leitor ao item 3.2.

[231] Entende-se que "A norma jurídica, no *direito do trabalho,* apresenta um dado que a difere das demais que integram o ordenamento jurídico. Não é de natureza formal, mas material. O seu conteúdo tem uma característica. É a *especialidade*, fator justificante da sua existência e característica que faz dela norma diferente das demais com as quais convive no sistema jurídico. A especialidade é compreendida como a qualidade que faz de algo um ser ou um fenômeno particular e inconfundível com outros, do mesmo ou de outro gênero, propriedade que apresenta a norma jurídica de *ser* no ordenamento jurídico, uma norma que não se confunde com as demais." (NASCIMENTO, 2011 p. 67).

[232] Segundo Goldschmidt (2019a, p. 132), "se houver uma fonte jurídica mais benéfica, seja ela uma norma, uma cláusula coletiva, uma súmula de jurisprudência, ainda que não tipicamente de direito do trabalho, mas compatível e adequada ao caso concreto, a mesma prevalecerá, em benefício do trabalhador, considerado hipossuficiente/vulnerável na relação de trabalho."

[233] Para maior aprofundamento acerca da figura da ANPD, remete-se o leitor ao item 3.4.

Em razão das infrações às normas da LGPD, os agentes de tratamento de dados estão sujeitos às penalidades de advertência, com indicação de prazo para adoção de medidas corretivas, ao pagamento de multa de até 2% do faturamento da empresa ou do grupo limitada, no total, a R$ 50 milhões por infração, à publicização da infração após devidamente apurada e confirmada a sua ocorrência, ao bloqueio dos dados pessoais correspondentes à infração até a sua regularização, além da eliminação dos dados pessoais correspondentes à infração, nos termos do artigo 52 da LGPD.

O § 1º do aludido dispositivo preconiza que todas as sanções serão precedidas de um procedimento administrativo que garanta a ampla defesa do infrator. Além disso, as sanções serão aplicadas considerando as particularidades de cada caso, bem como os seguintes parâmetros e critérios: a gravidade e a natureza das infrações e dos direitos pessoais afetados, a boa-fé do infrator, a vantagem auferida ou pretendida pelo infrator, a condição econômica do infrator, a reincidência, o grau do dano, a cooperação do infrator, a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, adoção de política de boas práticas e governança[234], a pronta adoção de medidas corretivas, e a proporcionalidade entre a gravidade da falta e a intensidade da sanção.[235]

Por fim, além de fixar a responsabilização dos agentes, a LGPD, orientada pelos princípios da prevenção e da segurança, se preocupou em estabelecer um conjunto de medidas técnicas e organizacionais a serem adotadas por aqueles que realizam o tratamento dos dados, as quais serão objeto de análise do próximo item.

---

[234] Com relação ao ponto, a doutrina adverte que “A mera elaboração de políticas de *compliance* que carecem de efeitos na prática corporativa – os chamados “programas de papel” – não consiste em mecanismo de efetivo autocontrole. Por consequência, a tendência é que sejam desconsiderados pelos órgãos regulatórios, sem que resultem na atenuação das sanções a serem aplicadas. Um “programa de fachada, que não preencha os requisitos mínimos ou que preencha apenas formalmente, pode de fato resultar em penalidades maiores do que aquelas que seriam aplicáveis em sua ausência.” (FRAZÃO; OLIVA; ABILIO, 2019, p. 686-687).

[235] Segundo o Parecer ao Projeto de Lei nº 4.060/2012, a fixação dos critérios e parâmetros permite melhor gradação das penas, trazendo circunstâncias atenuantes e agravantes que auxiliam na aplicação mais justa e equilibrada das sanções previstas. (CÂMARA DOS DEPUTADOS, 2018).

4.4 POLÍTICAS E PROCEDIMENTOS DA LEI Nº 13.709/2018 NA TUTELA DE DADOS

A transformação digital das empresas e a implementação de novas formas de controle por meios tecnológicos (vigilância por vídeo ou por *drones*, geolocalização, registro de dados biométricos, implantação de *microchips* em trabalhadores, a análise maciça de dados – *Big Data*, entre outros), como adiantado, aumentou o controle exercido pelo empregador, o qual pode entrar em conflito com direitos fundamentais dos trabalhadores, tais como a privacidade, a dignidade, o sigilo das comunicações, dentre outros.

Da mesma forma, quando essas novas tecnologias incluem a coleta e o processamento de dados, permitindo o exercício dos poderes de monitoramento e controle, surge a necessidade de se falar em políticas e procedimentos que assegurem a tutela dos dados pessoais e sensíveis dos trabalhadores, o que se caracteriza por um gerenciamento responsável dos dados por parte da empresa.

Nessa perspectiva, ganha relevo o princípio da prevenção, na medida em que uma das características da LGPD:

> [...] consiste no significativo fomento ao aspecto preventivo, estabelecendo procedimentos mandatórios para os controladores e operadores de dados pessoais, tais como os deveres atinentes à implementação de severas políticas de segurança para proteção dos dados de acessos não autorizados. Cuida-se de perspectiva alvissareira, na medida em que as características inerentes ao "meio digital" – entre elas a velocidade das transformações tecnológicas, a capacidade de propagação de informações e a dificuldade na contenção do fluxo de dados –, associadas à expansão da coleta e do tratamento implicam desafios à lógica repressiva, ainda mais quando esta decorre do modelo comando-controle. O engajamento espontâneo dos titulares dos deveres e a prevenção na tutela do direito fundamental aos dados pessoais afiguram-se essenciais e, não à toa, no que diz respeito a este último aspecto, cuida-se de princípio plasmado no art. 7º, VIII, da LGPD[236]. (FRAZÃO; OLIVA; ABILIO, 2019, p. 681).

Nesse sentido, o artigo 46 da Lei nº 13.709/2018 impõe aos responsáveis pelo tratamento dos dados a responsabilidade pela implementação de medidas de segurança. No caso da relação laboral, o agente que coleta e processa dados pessoais relacionados aos trabalhadores torna-se responsável pelo tratamento,

---

[236] Observa-se que, embora as autoras tenham referenciado o artigo 7º da LGPD, o princípio da prevenção encontra-se previsto no artigo 6º, inciso VIII.

devendo respeitar não apenas os princípios de coleta e processamento de dados, mas também, a adoção de:

> [...] medidas de segurança, técnicas e administrativas 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. (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

Verifica-se, ainda, que na esteira da regulamentação europeia (artigo 25 do RGPD), o § 2º do artigo 46 incorpora o conceito de privacidade desde a concepção (*privacy by design*): "As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução." (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

Como salientado, embora a LGPD não seja uma normativa específica em matéria de proteção de dados dos trabalhadores, as medidas nela estabelecidas, como as relativas à *avaliação de impacto sobre a proteção de dados* (AIPD), ao *registo das operações de tratamento*, à obrigação de indicar um *encarregado da proteção de dados* (EPD), bem como aos *selos, certificados e códigos de conduta regularmente emitidos*, são aplicáveis no âmbito laboral[237], por força do parágrafo primeiro do artigo 8ª da CLT, que admite a aplicação subsidiária e supletiva do direito comum.

Quanto à primeira medida, correspondente à *avaliação de impacto sobre a proteção de dados* (AIPD), com a adoção das novas tecnologias e dos recursos disponíveis, é possível que um tratamento de dados pessoais e sensíveis implique elevado risco para os direitos e liberdades dos trabalhadores. Nesse sentido:

> Uma AIPD é um processo concebido para descrever o tratamento, avaliar a necessidade e proporcionalidade desse tratamento e ajudar a gerir os riscos para os direitos e liberdades das pessoas singulares decorrentes do tratamento dos dados pessoais avaliando-os e determinando as medidas necessárias para fazer face a esses riscos. (GT29, 2017a, p. 04).

Frente a tal situação, o responsável pelo tratamento estará obrigado, antes de iniciar a sua tarefa, a realizar uma avaliação de impacto das operações sobre a proteção de dados dos trabalhadores. Disso decorre a importância de uma AIPD ser

---

[237] Quanto à incidência da LGPD no âmbito das relações de trabalho, remete-se o leitor ao item 3.2 para maior aprofundamento.

iniciada o mais cedo possível, mesmo que algumas das operações de tratamento ainda sejam desconhecidas.

> A atualização da AIPD ao longo do ciclo de vida do projeto garantirá que a proteção dos dados e a privacidade serão consideradas e incentivará a criação de soluções que promovem a conformidade. [...] O facto de a AIPD poder necessitar de ser atualizada após o tratamento ter efetivamente sido iniciado não é uma razão válida para adiar ou não realizar uma AIPD. A AIPD é um processo contínuo, especialmente quando uma operação de tratamento é dinâmica e está sujeita a mudanças permanentes. (GT29, 2017a, p. 17).

Além disso, por meio dessa medida, os responsáveis pelo tratamento devem descrever as operações e sua finalidade, as metodologias a serem utilizadas, a respectiva necessidade e proporcionalidade, os riscos para os direitos e liberdades dos titulares dos dados e as medidas essenciais para a sua mitigação.[238]

Tal obrigação constitui uma importante ferramenta complementar ao princípio da responsabilidade, na medida em que:

> [...] devendo a avaliação ter lugar num momento prévio ao tratamento, visa assegurar que a proteção de dados e privacidade sejam consideradas desde a concessão do processo de tratamento, promovendo, assim, a criação de soluções que assegurem o cumprimento das regras de proteção de dados e constituindo um elemento essencial para demonstrar tal cumprimento. (LOPES, 2018, p. 61).

Ressalta-se que a execução de uma avaliação de impacto não é obrigatória para todo o tipo de tratamento de dados pessoais, incidindo apenas quando o tratamento puder “gerar riscos às liberdades civis e aos direitos fundamentais”. Com relação ao tema, o GT29 esclarece que:

> [...] a referência aos “direitos e liberdades” dos titulares dos dados diz sobretudo respeito aos direitos de proteção dos dados e privacidade, mas também envolve outros direitos fundamentais como a liberdade de expressão, a liberdade de pensamento, a liberdade de circulação, a proibição de discriminação, o direito à liberdade, consciência e religião. [...] Contudo, o simples facto de as condições que conduzem à obrigação de realizar uma AIPD não terem sido satisfeitas não diminui a obrigação geral que os responsáveis pelo tratamento têm de aplicar medidas que visem gerir adequadamente os riscos para os direitos e as liberdades dos titulares dos dados. Na prática, tal significa que os responsáveis pelo tratamento devem

[238] Nesse sentido, dispõe o artigo 5º, inciso XVII que o relatório de impacto à proteção de dados pessoais refere-se à “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;” (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

> avaliar continuamente os riscos criados pelas suas atividades de tratamento por forma a identificarem quando um certo tipo de tratamento é "suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares". (GT29, 2017a, p. 07).

Ainda, existem circunstâncias em que o tratamento de dados é "suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares". Com relação a este ponto, o artigo 35, n. 3, do RGPD, refere, a título exemplificativo, algumas operações de tratamento em que a realização da AIPD será obrigatória:

> Artigo 35, n. 3. A realização de uma avaliação de impacto sobre a proteção de dados a que se refere o n. 1 é obrigatória nomeadamente em caso de:
> a) avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar;[239]
> b) operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9º, n. 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10;[240] ou
> c) controlo sistemático de zonas acessíveis ao público em grande escala. (UNIÃO EUROPEIA, 2016).

A fim de fornecer um conjunto mais concreto de operações de tratamento que exigem uma AIPD devido ao elevado risco inerente, o GT29 elenca nove critérios a serem considerados: 1) avaliação ou classificação;[241] 2) decisões automatizadas

---

[239] Segundo a parte final do considerando 71 do RGPD, "[...] o responsável pelo tratamento deverá utilizar procedimentos matemáticos e estatísticos adequados à definição de perfis, aplicar medidas técnicas e organizativas que garantam designadamente que os fatores que introduzem imprecisões nos dados pessoais são corrigidos e que o risco de erros é minimizado, e proteger os dados pessoais de modo a que sejam tidos em conta os potenciais riscos para os interesses e direitos do titular dos dados e de forma a prevenir, por exemplo, efeitos discriminatórios contra pessoas singulares em razão da sua origem racial ou étnica, opinião política, religião ou convicções, filiação sindical, estado genético ou de saúde ou orientação sexual, ou a impedir que as medidas venham a ter tais efeitos. A decisão e definição de perfis automatizada baseada em categorias especiais de dados pessoais só deverá ser permitida em condições específicas. (UNIÃO EUROPEIA, 2016).

[240] O considerando 75 do RGPD menciona algumas situações em que pode haver risco para os direitos e liberdades das pessoas singulares: quando forem tratados dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas e a filiação sindical, bem como dados genéticos ou dados relativos à saúde ou à vida sexual ou a condenações penais e infrações ou medidas de segurança conexas; ou quando o tratamento incidir sobre uma grande quantidade de dados pessoais e afetar um grande número de titulares de dados. (UNIÃO EUROPEIA, 2016).

[241] Inclui "definição de perfis e previsão, em especial de *'aspetos relacionados com o desempenho profissional, a situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados*.' Por exemplo: uma empresa de biotecnologia que ofereça testes genéticos diretamente aos seus clientes por forma a avaliar e prever riscos de doença ou para a saúde. (GT29, 2017a, p. 10).

que produzam efeitos jurídicos ou afetem significativamente de modo similar;[242] 3) controlo sistemático;[243] 4) dados sensíveis ou dados de natureza altamente pessoal;[244] 5) dados tratados em grande escala;[245] 6) estabelecer correspondências ou combinar conjuntos de dados;[246] 7) dados relativos a titulares de dados vulneráveis;[247] 8) utilização de soluções inovadoras ou aplicação de novas soluções

---

[242] "Tratamento destinado à tomada de decisões sobre os titulares dos dados e que produza '*efeitos jurídicos relativamente à pessoa singular'* ou que 'a afetem significativamente de forma similar'." Por exemplo: o tratamento pode implicar a exclusão ou a discriminação de indivíduos. (GT29, 2017a, p. 10).

[243] "Tratamento utilizado para observar, monitorizar ou controlar os titulares dos dados, incluindo dados recolhidos através de redes, ou um '*controlo sistemático de zonas acessíveis ao público'.* [...] Este tipo de controlo é um critério porque os dados pessoais podem ser recolhidos em circunstâncias em que os titulares dos dados podem não estar cientes de quem está a recolher os seus dados e da forma como esses dados serão utilizados. Adicionalmente, pode ser impossível para os indivíduos evitarem estar sujeitos a este tipo de tratamento em espaço(s) público(s) (ou zonas acessíveis ao público)." (GT29, 2017a, p. 11).

[244] Inclui categorias especiais de dados pessoais (por exemplo, informações acerca das opiniões políticas dos indivíduos), bem como dados pessoais relacionados com condenações penais e infrações. "Um exemplo seria um hospital geral que mantenha registos médicos dos doentes ou um investigador privado que mantenha informações acerca dos autores das infrações. Para além destas disposições do RGPD, algumas categorias de dados podem ser consideradas como categorias que aumentam os possíveis riscos para os direitos e as liberdades dos indivíduos. Estes dados pessoais são considerados sensíveis (na aceção comum deste termo) porque estão associados a atividades privadas e familiares (tais como comunicações eletrónicas cuja confidencialidade deve ser protegida) ou porque afetam o exercício de um direito fundamental (tais como dados de localização cuja recolha põe em causa a liberdade de circulação) ou porque a sua violação implica claramente que a vida quotidiana do titular dos dados será gravemente afetada (tais como dados financeiros que possam ser utilizados numa fraude de pagamentos). A este respeito, pode ser relevante saber se os dados já foram tornados públicos pelo titular dos dados ou por terceiros. O facto de os dados pessoais já terem sido tornados públicos pode ser considerado um fator pertinente para avaliar se, possivelmente, os dados seriam ou não utilizados para determinados fins. Este critério pode também incluir dados como documentos pessoais, mensagens de correio eletrónico, diários, notas de dispositivos eletrónicos de leitura equipados com funções de introdução de notas, bem como informações muito pessoais incluídas em aplicações onde ficam registados eventos da vida dos indivíduos." (GT29, 2017a, p. 11).

[245] Não há definição no RGPD, tampouco na LGPD, do que constitui grande escala, contudo o GT29 "recomenda que os seguintes fatores, em especial, sejam considerados quando se determina se o tratamento é ou não efetuado em grande escala: a. o número de titulares de dados envolvidos, quer através de um número específico quer através de uma percentagem da população pertinente; b. o volume de dados e/ou a diversidade de dados diferentes a tratar; c. a duração da atividade de tratamento de dados ou a sua pertinência; d. a dimensão geográfica da atividade de tratamento." (GT29, 2017a, p. 11-12).

[246] "Por exemplo, com origem em duas ou mais operações de tratamento de dados realizadas com diferentes finalidades e/ou por diferentes responsáveis pelo tratamento de dados de tal forma que excedam as expectativas razoáveis do titular dos dados." (GT29, 2017a, p. 12).

[247] "O tratamento deste tipo de dados constitui um critério devido ao acentuado desequilíbrio de poder entre os titulares dos dados e o responsável pelo tratamento dos dados, significando isto que os indivíduos podem não ser capazes de consentir, ou opor-se, facilmente ao tratamento dos seus dados ou de exercer os seus direitos. Os titulares de dados vulneráveis podem incluir crianças (estas podem ser consideradas incapazes de consentir ou opor-se consciente e criteriosamente ao tratamento dos seus dados), empregados, segmentos mais vulneráveis da população que necessitem de proteção especial (pessoas com doenças mentais, requerentes de asilo, idosos, doentes, etc.) e todos os casos em que possa ser identificado um desequilíbrio na relação entre a posição do titular dos dados e o responsável pelo tratamento." (GT29, 2017a, p. 12).

tecnológicas ou organizacionais;[248] 9) quando o próprio tratamento *impede os titulares dos dados* "*de exercer um direito ou de utilizar um serviço ou um contrato"*[249].

Diante disso, o responsável pelo tratamento de dados pode considerar que um tratamento que satisfaça dois critérios exige a realização de uma AIPD, ou pode considerar que um tratamento que satisfaça apenas um dos critérios exige a realização de uma AIPD, ou então considerar que embora presentes os critérios, a operação não é "suscetível de implicar um elevado risco", hipótese em que terá que justificar e documentar as razões que o conduzirão a não realizar uma AIPD. Contudo, no entender do GT29:

> [...] quantos mais critérios forem satisfeitos pelo tratamento maior é a probabilidade de este implicar um elevado risco para os direitos e as liberdades dos titulares dos dados e, por conseguinte, de necessitar de uma AIPD, independentemente das medidas que o responsável pelo tratamento pretender adotar. (GT29, 2017a, p. 12).

Partindo disso, o GT29 apresenta alguns exemplos que ilustram a forma como os critérios devem ser utilizados para avaliar se uma operação de tratamento específica exige ou não uma AIPD: 1º exemplo de tratamento – uma empresa que controle sistematicamente as atividades dos seus empregados, incluindo o controle dos computadores e da atividade *internet* dos seus empregados. Critérios pertinentes possíveis: controle sistemático + dados relativos a titulares de dados vulneráveis. Exige-se a realização de uma AIPD? Sim. 2º exemplo de tratamento – recolha de dados públicos das redes sociais para elaborar perfis. Critérios pertinentes possíveis: avaliação ou classificação + dados tratados em grande escala + estabelecer correspondências ou combinar conjuntos de dados + dados sensíveis ou dados de natureza altamente pessoal. Exige-se a realização de uma AIPD? Sim.

---

[248] Trata-se, por exemplo, de "combinar a utilização da impressão digital e do reconhecimento facial para melhorar o controlo do acesso físico, etc. [...] a utilização de uma nova tecnologia, definida em '*conformidade com o nível de conhecimentos tecnológicos alcançado'* [...], pode desencadear a necessidade de realização de uma AIPD. Isto acontece porque a utilização dessa tecnologia pode envolver novas formas de recolha e utilização de dados, possivelmente com elevado risco para os direitos e as liberdades dos indivíduos. Na verdade, as consequências pessoais e sociais da implantação de uma nova tecnologia podem ser desconhecidas. Uma AIPD ajudará o responsável pelo tratamento de dados a compreender e dar resposta a esses riscos. Por exemplo, algumas aplicações da 'Internet das Coisas' podem ter um impacto significativo na vida quotidiana e na privacidade dos indivíduos e, como tal, exigem a realização de uma AIPD. (GT29, 2017a, p. 12).

[249] "Estão incluídas operações de tratamento destinadas a autorizar, alterar ou recusar o acesso dos titulares dos dados a um serviço ou que estes celebrem um contrato. Um exemplo disto é quando um banco faz um controlo seletivo dos seus clientes a partir de uma base de dados de referências de crédito bancário com vista a decidir se lhes concede ou não um empréstimo." (GT29, 2017a, p. 12).

Adicionalmente, a LGPD prevê a possibilidade de a autoridade nacional solicitar ao responsável pelo tratamento que elabore relatório de impacto à proteção de dados pessoais, inclusive sensíveis, observados os segredos comercial e industrial (artigo 38 da LGPD).

Além disso, haverá situações, segundo o GT29, em que a AIPD não será obrigatória: a) quando o tratamento não for "*suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares"*; b) quando já existir uma AIPD semelhante; c) quando tiver sido autorizado antes de maio de 2018[250] (mês de entrada em vigor do RGPD); d) quando tiver um fundamento jurídico ou quando fizer parte de uma lista de operações de tratamento para as quais não seja necessária uma AIPD. (GT29, 2017a, p. 14-15).

Ainda, como parte do princípio da responsabilização, cada responsável pelo tratamento de dados deve conservar um *registro de todas as atividades de tratamento* sob sua responsabilidade, a qual corresponde à segunda medida. Nesse sentido, a LGPD, dispõe no artigo 37: "o controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse." (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

Na sequência, assim como o RGPD, a LGPD institui a figura do *encarregado da proteção de dados* (EPD)[251] como um elemento chave no novo modelo de governação, o qual assume um papel central no cumprimento por parte das instituições das disposições legais relativas à proteção de dados pessoais.

---

[250] O GT29 refere que "mesmo que não seja obrigatória a realização de uma AIPD em 25 de maio de 2018, será necessário, na altura adequada, que o responsável pelo tratamento realize essa AIPD como parte das suas obrigações gerais em matéria de responsabilização." Tal necessidade decorre, uma vez que pode haver mudança nas condições que ensejaram o tratamento de dados. "Além disso, pode ser obrigatório realizar uma AIPD após uma alteração dos riscos decorrentes das operações de tratamento, por exemplo, porque se começou a utilizar uma nova tecnologia ou porque os dados pessoais passaram a ser utilizados para uma finalidade diferente. As operações de tratamento de dados podem evoluir rapidamente e podem surgir novas vulnerabilidades. [...] Uma AIPD também pode tornar-se necessária pelo facto de o contexto organizacional ou societal da atividade de tratamento ter mudado, por exemplo, porque os efeitos de determinadas decisões automatizadas se tornaram mais significativos ou porque novas categorias de titulares de dados ficaram vulneráveis a discriminação. Cada um destes exemplos pode ser um elemento que conduz a uma alteração do risco decorrente da atividade de tratamento em causa." (GT29, 2017a, p. 16).

[251] Dada a importância do papel exercido pelos encarregados da proteção de dados (EPD) quanto ao cumprimento das disposições do RGPD, o Grupo do Artigo 29º para a Proteção de Dados (GT29) editou um conjunto de orientações sobre os EPD, cujas diretrizes podem servir de fonte para a LGPD brasileira, naquilo em que for compatível, dada a similitude das normativas.

Segundo o GT29, “os EPD devem igualmente dispor de autonomia e de recursos suficientes para desempenhar eficazmente as suas funções.” (GT29, 2017b, p. 06).

De acordo com o artigo 5º, inciso VIII, da LGPD, o EPD corresponde à “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).” (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

A fim de assegurar que o EPD se encontre acessível, o § 1º do artigo 41 da LGPD prevê que a sua identidade e as informações do seu contato devem ser divulgadas publicamente, de forma clara e objetiva. Além disso, o § 2º do mencionado dispositivo dispõe que as atividades do encarregado consistem em:

> I – aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II – receber comunicações da autoridade nacional e adotar providências; III – orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV – executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares. (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

Verifica-se, portanto, que o encarregado tem papel fundamental na promoção de uma cultura de *compliance* na área de proteção de dados dentro da organização para a qual trabalha.[252] O § 3º do artigo 41 da LGPD também prevê a possibilidade de a autoridade nacional dispensar a necessidade de indicação do encarregado, a depender da “natureza e o porte da entidade ou o volume de operações de tratamento de dados.” (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

E, ainda, quanto aos EPD, o GT29 sinaliza que, não obstante sejam responsáveis por zelar pela implementação e cumprimento das regras de proteção de dados, eles não são pessoalmente responsáveis em caso de descumprimento. Na verdade, ao abrigo do princípio da responsabilidade, a designação do encarregado não exonera os agentes de tratamento (controlador e operador) da responsabilidade em assegurar e demonstrar a conformidade com as disposições da lei.[253]

---

[252] Quanto ao tema do *compliance*, remete-se o leitor ao item 4.2.

[253] Nesse sentido, o artigo 43 da LGPD dispõe que “Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem: [...] II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados;” (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

No que tange aos *selos de proteção, à certificação e aos códigos de conduta*,[254] estes também estão previstos no artigo 33, II, "d", e artigo 35, ambos da LGPD. Trata-se de instrumentos que, além de auxiliarem na demonstração do cumprimento das obrigações pelo responsável pelo tratamento, atuam como fator atenuante na aplicação de sanções (artigo 52, § 1º, VIII, da LGPD).

Por conseguinte, salienta-se que a Lei nº 13.709/2018, cuja entrada em vigor está prevista para agosto de 2020, a exemplo do que ocorreu na União Europeia, se apresenta como um instrumento essencial para a modernização das regras de proteção de dados no Brasil, especialmente frente aos novos desafios da era digital.

Como destacado, as ferramentas tecnológicas favorecem a utilização de dados pessoais e sensíveis em grande escala, o que também se reflete no ambiente de trabalho, surgindo a necessidade da construção de um quadro de proteção de dados sólido e eficaz, que respeite os direitos e liberdades fundamentais da pessoa-trabalhadora.

Portanto, inegável a relevância da recém aprovada LGPD no Brasil, a qual, afinada com as questões advindas da chamada revolução tecnológica, configura um importante instrumento para este *Admirável Mundo Novo do Trabalho*[255], especialmente pelo seu caráter principiológico, pelo fomento à implementação de uma cultura de *compliance*, bem como pelo estabelecimento de medidas técnicas e organizativas, as quais, em conjunto, contribuirão para uma eficaz e efetiva proteção dos dados pessoais e sensíveis dos trabalhadores.

---

[254] De acordo com considerandos 98 e 99 do RGPD, os códigos de conduta representam mecanismos de autorregulação suscetíveis de conferir orientação sobre a aplicação efetiva das regras de proteção de dados, tendo em conta as especificidades de cada setor e as necessidades das micro, pequenas e médias empresas. O considerando 100 do RGPD, por sua vez, estabelece que "a fim de reforçar a transparência e o cumprimento do presente regulamento, deverá ser encorajada a criação de procedimentos de certificação e selos e marcas de proteção de dados, que permitam aos titulares avaliar rapidamente o nível de proteção de dados proporcionado pelos produtos e serviços em causa. (UNIÃO EUROPEIA, 2016).

[255] A expressão "Admirável Mundo Novo do Trabalho" foi adotado como título de um artigo escrito pela Professora Doutora Teresa Alexandra Coelho Moreira, da Universidade do Minho, no qual a autora (2012) explica ter se utilizado do nome da obra de ULRICH BECK, *The Brave New World of Work*, Polity Press, Oxford, 2000, que se inspirou no livro de ALDOUS HUXLEY, O *Admirável Mundo Novo*, Colecção Mil Folhas, Lisboa, 2003, na medida em que entende que as novas tecnologias revolucionaram a concepção que tinha do mundo. (MOREIRA, 2012, p. 15). Para uma leitura mais aprofundada sobre o tema, remete-se o leitor ao item 2.2 e 2.4.

7 CONCLUSÃO

A rápida evolução tecnológica, a globalização e o fenômeno do *big data* estão desencadeando uma série de apreensões para o mundo do trabalho. Fala-se cada vez mais em Trabalho 4.0, em revolução digital e seus efeitos sobre as relações laborais. Contudo, o futuro do Direito do Trabalho já é uma realidade vivenciada pela sociedade. O momento atual é de mudanças disruptivas, sendo necessária, mais do que nunca, uma revitalização do contrato social que seja centrado na pessoa humana, e que garanta um trabalho digno e decente em escala mundial, tal como prevê a Declaração do Centenário da OIT.

Hoje, discute-se gradativamente sobre inteligência artificial, *cloud computer*, impressoras 3D, robótica, geolocalização, controle eletrônico, *colaborative robots*, dentre outros, e seus impactos no futuro do trabalho. No tocante, dois temas chamam a atenção: o primeiro, refere-se ao temor do desemprego tecnológico frente à mudança do processo produtivo; o segundo, trata do aumento significativo da coleta e armazenamento de dados pessoais da pessoa-trabalhadora e a sua utilização em grande escala pelas empresas no exercício das suas atividades.

Com relação ao primeiro aspecto, inegável que as transformações do mundo digital estão transformando os padrões de atividade, de interação humana e o ritmo da produção, tal como ocorreu no passado com as revoluções industriais anteriores. A grande diferença é que com a indústria 4.0, a velocidade e o alcance das mudanças são significativamente maiores, logo o receio da automatização dos empregos é premente.

Por outro lado, profissões mais especializadas tendem a surgir, assim como novas formas de prestação de trabalho já são perceptíveis, a exemplo da chamada *gig economy,* a qual vem se expandindo nos últimos anos. Assim, entende-se que a preocupação maior não deve ser quanto ao desemprego tecnológico, mas quanto à qualidade dos trabalhos que serão criados, havendo a necessidade de se repensar o Direito do Trabalho, sem esquecer a sua base centrada na proteção da pessoa humana do trabalhador.

Paralelo a isso, as mudanças advindas requerem o envolvimento dos Estados, das instituições internacionais, das associações empresariais e das organizações sindicais, a fim de evitar ou minimizar as consequências negativas.

Logo, a educação universal e a formação contínua surgem como instrumentos chave para capacitar os trabalhadores frente à entrada da indústria 4.0.

Quanto aos trabalhadores em condição social mais fragilizada, incluindo os de idade avançada, os jovens sem experiência e os trabalhadores que carecem de formação, a fim de assegurar uma proteção, ainda que mínima, e reduzir as desigualdades promovidas pela revolução tecnológica, defende-se a concessão de um renda básica universal, de modo que tais pessoas possam viver com dignidade e satisfazer suas necessidades mais essenciais, sem cair em situação de pobreza ou de exclusão social.

Quanto ao segundo aspecto, o qual corresponde ao tema central da presente pesquisa, as NTIC transformaram a economia e a vida social, a ponto de resultar em uma sociedade gradativamente orientada por dados, também conhecida como a era datacêntrica ou dataísmo. Consequentemente surge a necessidade de se construir um quadro de proteção de dados sólido e efetivo, que traga segurança jurídica, e que permita que as pessoas possam controlar a utilização que é feita dos seus dados pessoais e sensíveis.

No âmbito das relações de trabalho, a utilização massiva das novas ferramentas tecnológicas tem ampliado o exercício do poder de controle, dando origem ao chamado controle eletrônico do empregador. Por meio deste, é possível à distância e em tempo real reunir informações diversas sobre a pessoa do trabalhador, inclusive sobre múltiplas facetas da sua vida, tais como seus gostos, preferências, interesses, prevendo até mesmo a sua forma de pensar.

Todavia, tal poder de controle do empregador vem gerando tensões, pois nem tudo que é tecnicamente possível, é juridicamente admissível. Embora o empregador tenha legitimidade para exercer o poder diretivo, este não pode conduzir a uma reificação da pessoa humana. É preciso lembrar que o trabalho não é uma mercadoria, que pode ser separado da pessoa que o presta. Os trabalhadores, antes de tudo, são pessoas com direitos, necessidades e aspirações. Além disso, o que encontra-se à disposição do empregador é a sua força de trabalho e não a sua pessoa.

Nesse sentido, os direitos e liberdades fundamentais dos trabalhadores emergem como limites ao legítimo direito do empregador de dirigir e controlar as tarefas daqueles. Entender de outro modo, pode conduzir a um desaparecimento parcial ou total dos direitos fundamentais inespecíficos, tais como a privacidade, a liberdade e a própria dignidade dos trabalhadores. Vale lembrar que o trabalhador é

um sujeito e não um objeto, de forma que as ferramentas tecnológicas é que devem adaptar-se, e não o contrário, sob pena de haver quebra da confiança mútua que deve permear as relações de trabalho.

Soma-se a isso o fato de que o uso irrestrito e abusivo das ferramentas tecnológicas tem produzido novas formas de exclusão que são ainda mais radicais, pois permitem identificar aspectos relacionados à vida privada trabalhador, atingindo até mesmo aspectos ligados à vida social, sexual, familiar e afetiva, os quais serão levados em consideração nos processos de seleção, nos programas de ascensão funcional, nas premiações e nos processos de dispensa.

Evidente que para o trabalhador torna-se difícil resistir, primeiro porque muitas vezes nem toma conhecimento das práticas adotadas pela empresa, segundo porque, muito embora possa se opor, a realidade do mercado de trabalho, caracterizado por contrato frágeis e sem segurança, somado aos altos índices de desemprego, faz com que o trabalhador não apresente resistência, ainda que as informações coletadas nada avaliem a aptidão profissional em si.

Com efeito, observa-se que os direitos fundamentais dos trabalhadores correm sério risco, seja pela falta de proteção social, seja pela crescente precarização das relações laborais, seja porque o controle total direto e à distância, espacial e temporal, é constante, seja porque cada vez mais sentem dificuldade em separação as fronteiras entre a vida pessoal e a vida profissional.

Nessa perspectiva, para conter os riscos reais e potenciais do mau uso ou do uso abusivo das tecnologias de informação e armazenamento digital, assume especial relevância a proteção dos dados pessoais e sensíveis, como direito fundamental do trabalhador brasileiro, no contexto da sociedade da informação, caracterizada pelo uso intensivo de novas tecnologias.

Com base nisso, o tema da proteção de dados ganhou relevo mais recentemente, após a aprovação pelo Parlamento Europeu do Regulamento Geral de Proteção de Dados da União Europeia (RGPD) ou *General Data Protection Regulation* (GDPR), o qual entrou em vigor em 25 de maio de 2018. Trata-se da mais importante normativa sobre o tema da proteção de dados em âmbito mundial. No tocante ao Brasil, a legislação referente à proteção dos dados pessoais somente foi aprovada em 2018, inspirada no RGPD, a qual tem previsão de entrada em vigor em 2020.

Todavia, importante salientar que a LGPD foi elaborada visando assegurar uma proteção aos dados pessoais dos consumidores, sem previsão regulatória no

tocante aos dados pessoais dos trabalhadores. Assim, embora inexista um marco regulatório específico, dando tratamento detalhado e adequado à proteção dos dados pessoais e sensíveis do trabalhador no âmbito das relações de trabalho, defende-se a aplicação do chamado *microssistema jurídico de direitos da personalidade do trabalhador*, como forma de assegurar uma proteção a esses dados, entendidos como bens extrapatrimoniais da pessoa-trabalhadora, tuteláveis juridicamente.

À vista disso, uma vez que os dados pessoais e sensíveis refletem uma das múltiplas expressões da personalidade do trabalhador no âmbito das relações trabalhistas, fundamental que se construa um sistema de promoção e defesa desses dados, sendo que os princípios da LGPD, somados aos do Direito do Trabalho, o que inclui as disposições do Repertório de Recomendações Práticas da OIT sobre a Proteção de Dados Pessoais dos Trabalhadores, podem servir como guia para a construção de uma normativa específica para o setor laboral brasileiro.

Ainda com relação aos dados pessoais e sensíveis dos trabalhadores, tem-se que o direito à proteção desses dados não é absoluto, contudo, é fundamental se trabalhar com uma perspectiva preventiva, pois é muito mais difícil recuperar um dado violado do que defendê-lo de uma primeira violação. Dessa maneira, defende-se, ao lado da teoria da eficácia horizontal dos direitos fundamentais, a aplicação dos princípios da boa-fé objetiva e da proporcionalidade, os quais servirão como norte para a atividade de tratamento dos dados dos trabalhadores.

Paralelo a isso, os programas de *compliance* em matéria de proteção de dados, também denominados de programas de governança em privacidade, funcionam como importante instrumento operacional e preventivo da ocorrência de violações aos direitos dos titulares, na medida em que orientam os agentes de tratamento, traduzindo para suas atividades cotidianas as premissas principiológicas da LGPD e concretizando vários dos seus conceitos abertos. Ainda com relação a tais programas, a sua implementação pode ocorrer tanto em pequenas empresas como em grandes companhias, inclusive aquelas que operam nos meios digitais.

A responsabilidade do empregador quanto ao tratamento dos dados pessoais e sensíveis dos trabalhadores é outro ponto que merece destaque. A LGPD foi silente quanto à responsabilidade civil do empregador pelos danos causados aos titulares dos dados (trabalhadores). Apesar disso, os artigos 223-A a 223-G da CLT disciplinaram a reparação civil por danos extrapatrimoniais, sendo que o artigo 223-A inaugura uma espécie de *microssistema de responsabilidade civil por danos*

extrapatrimoniais no âmbito das relações laborais. Nesse sentido, como indicado, o artigo 223-C da CLT prevê um rol aberto de bens extrapatrimoniais juridicamente tuteláveis, a partir do qual é possível extrair a proteção aos dados pessoais e sensíveis dos trabalhadores.

Assim, do cotejo entre a LGPD e a CLT, bem como frente à especialidade do ramo laboral, defende-se a aplicação do novel regime dos artigos 223-A a 223-G da CLT às situações nas quais o empregador causar danos em razão do exercício de atividade de tratamento de dados pessoais e sensíveis dos trabalhadores.

Por fim, vale lembrar que, quando se fala em dados pessoais e sensíveis, a sua tutela é essencial para a proteção da pessoa humana, ainda que no exercício de atividade laboral, pois enquanto pessoa-trabalhadora, a condição humana não desaparece. Daí a importância de se melhorar as disposições de proteção especificamente dirigidas à utilização de dados pessoais e sensíveis dos trabalhadores, de modo a salvaguardar a sua dignidade, proteger a sua privacidade e garantir seu direito fundamental de determinar dados, bem como os propósitos e condições de uso.

REFERÊNCIAS

ABRANTES, José João. **Direitos fundamentais da pessoa humana no trabalho**: em especial, a reserva da intimidade da vida privada (algumas questões). Coimbra: Almedina, 2014. Edição do *Kindle*.

AGUIAR, Antonio Carlos. **Direito do trabalho 2.0**: digital e disruptivo. São Paulo: LTr, 2018.

AGUIAR, Antonio Carlos. Eu, o Robô e o Trabalho em Mutação: Antes, Agora e Depois. *In*: AGUIAR, Antonio Carlos. **Direito do trabalho 2.0**: digital e disruptivo. São Paulo: LTr, 2018. p. 67-104.

ALEXY, Robert. **Teoria dos direitos fundamentais**. Tradução Virgílio Afonso da Silva. São Paulo: Malheiros, 2008.

AMARAL, Júlio Ricardo de Paula. A intimidade privada e o direito à autodeterminação informativa. Um passo adiante para a efetiva proteção das informações pessoais dos trabalhadores. **Revista Tribunal Regional do Trabalho da 9ª Região**. Curitiba, ano 40, n. 72, p. 247-341, jan./dez. 2015.

ANDRADE, Flávio Carvalho Monteiro de; FERREIRA, Isadora Costa. *Compliance* trabalhista: compreendendo a prevenção de risco trabalhista por meio de programa de integridade. **Revista Síntese**: trabalhista e previdenciária. São Paulo, v. 28, n. 331, p. 73-84, jan. 2017.

ANTONIK, Luis Roberto. **Compliance, ética, responsabilidade social e empresarial**: uma visão prática. Rio de Janeiro: Alta Books, 2016. Edição do *Kindle*.

ANTUNES, Ricardo. **O privilégio da servidão**: o novo proletariado de serviços na era digital. 1. ed. São Paulo: Boitempo, 2018. *E-Book*.

APOSTOLIDES, Sara Costa. Do dever de informação do trabalhador. *In*: APOSTOLIDES, Sara Costa. **Do dever pré-contratual de informação e da sua aplicabilidade na formação do contrato de trabalho**. Coimbra: Almedina, 2008. p. 211-255.

APOSTOLIDES, Sara Costa. **Do dever pré-contratual de informação e da sua aplicabilidade na formação do contrato de trabalho**. Coimbra: Almedina, 2008.

APP. *In*: **Dicionário Priberam da Língua Portuguesa**. Disponível em: https://dicionario.priberam.org/app. Acesso em: 05 set. 2019.

ASSOCIAÇÃO NACIONAL DOS MAGISTRADOS DA JUSTIÇA DO TRABALHO (ANAMATRA). **Congressos nacionais dos magistrados da justiça do trabalho**: a história dos Conamats (1ª a 17ª edições), Brasília, 2015. Disponível em: https://www.anamatra.org.br/images/conamat/Cadernos_Anamatra_Conamats_site.pdf. Acesso em: 25 ago. 2018.

BAEZ, Narciso Leandro Xavier; MOZETIC, Vinicius Almada; MARTIN, Nuria Belloso; SÁNCHEZ, Helena Nadal. (org.). **O impacto das novas tecnologias nos direitos fundamentais**. Joaçaba: Unoesc, 2018.

BARROS, Alice Monteiro. **Curso de direito do trabalho**. 10. ed. São Paulo: LTr, 2016.

BARROSO, Luís Roberto. **Curso de direito constitucional contemporâneo:** os conceitos fundamentais e a construção do novo modelo. 2. ed. São Paulo: Saraiva, 2010.

BBC NEWS Brasil. Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. **BBC News Brasil**, 20 mar. 2018. Disponível em: https://www.bbc.com/portuguese/internacional-43461751. Acesso em: 21 ago. 2019.

BENÍTEZ, Esperanza Macarena Sierra. **¿Por qué debemos iniciar el debate sobre la necesidad de la implantación de una renta básica universal?** 2019. Disponível em: http://www.cielolaboral.com/por-que-debemos-iniciar-el-debate-sobre-la-necesidad-de-la-implantacion-de-una-renta-basica-universal/. Acesso em: 13 jul. 2019.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BITTAR, Carlos Alberto. **Reparação civil por danos morais**. 4 ed., rev., aum. e mod. por Eduardo C. B. Bittar. São Paulo: Saraiva, 2015.

BLUM, Renato Opice; ZAMPERLIN, Emelyn. Compliance, responsabilidade empresarial e segurança da informação. **Lex Magister**, Porto Alegre, 23 jun. 2016. Disponível em: https://www.lex.com.br/doutrina_27159943_COMPLIANCE_RESPONSABILIDADE_EMPRESARIAL_E_SEGURANCA_DA_INFORMACAO.aspx. Acesso em: 26 out. 2019.

BODIN DE MORAES, Maria Celina; MULHOLLAND Caitlin (org.). **Privacidade hoje**: Anais do I Seminário de Direito Civil da PUC-RIO. Rio de Janeiro: PUC-RIO, 2018. *E-book.* Disponível em: https://ler.amazon.com.br/?asin=B07FCQBCDB. Acesso em: 07 set. 2019.

BOLZAN DE MORAIS, Jose Luis; JACOB NETO, Elias. O que é isto, a *surveillance*? Direito e fluxos de dados globais no século XXI. *In*: BAEZ, Narciso Leandro Xavier; MOZETIC, Vinicius Almada; MARTIN, Nuria Belloso; SÁNCHEZ, Helena Nadal. (org.). **O impacto das novas tecnologias nos direitos fundamentais**. Joaçaba: Unoesc, 2018. p. 85-104.

BRANCO, Paulo Gustavo Gonet. O direito fundamental da privacidade nas relações de trabalho. *In*: SARLET, Ingo Wolfgang; MELLO FILHO, Luiz Philippe de; FRAZÃO, Ana de Oliveira. (coord.). **Diálogos entre o direito do trabalho e o direito constitucional**: estudos em homenagem a Rosa Maria Weber. São Paulo: Saraiva,

2014. p. 331-353.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 23 ago. 2019.

BRASIL. **Decreto-lei nº 5.452, de 1º de maio de 1943**. Aprova a Consolidação das Leis do Trabalho. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del5452compilado.htm. Acesso em: 21 jul. 2019.

BRASIL. **Lei Complementar nº 105, de 10 de janeiro de 2001**. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm. Acesso em: 09 set. 2019.

BRASIL. **Lei 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L8078compilado.htm. Acesso em: 03 set. 2019.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm. Acesso em: 06 set. 2019.

BRASIL. **Lei 12.414, de 9 de junho de 2011**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm. Acesso em: 09 set. 2019.

BRASIL. **Lei 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 09 set. 2019.

BRASIL. **Lei 12.846, de 1º de agosto de 2013**. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/L12846.htm. Acesso em: 14 out. 2019.

BRASIL. **Lei 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: 03 set. 2019.

BRASIL. **Lei 13.103, de 2 de março de 2015**. Dispõe sobre o exercício da profissão de motorista; altera a Consolidação das Leis do Trabalho - CLT, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943, e as Leis n º 9.503, de 23 de setembro de 1997 - Código de Trânsito Brasileiro, e 11.442, de 5 de janeiro de 2007 (empresas e transportadores autônomos de carga), para disciplinar a jornada de trabalho e o tempo de direção do motorista profissional; altera a Lei nº 7.408, de 25 de novembro de 1985; revoga dispositivos da Lei nº 12.619, de 30 de abril de 2012; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13103.htm. Acesso em: 01 nov. 2019.

BRASIL. **Lei 13.105, de 16 de março de 2015**. Código de Processo Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 23 out. 2019.

BRASIL. **Lei 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/_Ato2015-2018/2018/Lei/L13709compilado.htm. Acesso em: 27 ago. 2019.

BRITTO, Nara Pinheiro Reis Ayres de; RIBEIRO, Alanna Muniz. *Soft law* e *hard law* como caminho para afirmação do direito à proteção de dados: uma análise da experiência internacional e brasileira. *In:* FERNANDES, Ricardo Vieira de Carvalho; CARVALHO, Angelo Gamba Prata de (coord.). **Tecnologia jurídica & direito digital**: II Congresso Internacional de Direito, Governo e Tecnologia – 2018. Belo Horizonte: Fórum, 2018. p. 383-392.

CACHAPUZ, Maria Cláudia Mércio. Privacidade, proteção de dados e autodeterminação informativa. **Revista Jurídica da Presidência**, Brasília, v. 15, n. 107, p. 823-848, out./jan. 2014.

CÂMARA DOS DEPUTADOS. **Parecer ao Projeto de Lei nº 4.060/2012**. **Dispõe sobre o tratamento de dados pessoais e dá outras providências.** Brasília: Câmara dos Deputados, 24 maio 2018. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=PRL+1+PL406012+%3D%3E+PL+4060/2012. Acesso em: 23 out. 2019.

CAMARGO, Coriolano Almeida; SANTOS, Cleorbete. **Fundamentos do *Compliance***. 2019. Edição do *Kindle.*

CANO, Edgar Salazar. El derecho de la informática (una nueva especialidad juridica en la sociedade informatizada). **Anuario del Instituto de Derecho Comparado de la Facultad de Ciencias Jurídicas y Políticas de la Universidad de Carabobo**, Venezuela, n. 18, 1994. Disponível em: http://servicio.bc.uc.edu.ve/derecho/revista/idc18/18-14.pdf. Acesso em: 25 ago. 2019.

CANOTILHO, José Joaquim Gomes. **Direito Constitucional e Teoria da Constituição**. 7. ed. Coimbra, Portugal: Almedina, 2003.

CARVALHO, Luis Fernando Silva de. A tutela jurisdicional específica dos direitos da personalidade do trabalhador. *In*: GOLDSCHMIDT, Rodrigo. **Direitos da personalidade do trabalhador.** Rio de Janeiro: Lumen Juris, 2019, p. 227-248.

CARVALHO, Victor Miguel Barros de; GUIMARÃES, Patrícia Borba Vilar Guimarães; OLIVEIRA, Adriana Carla Silva de. A monetização de dados pessoais como alternativa a períodos de crise: análise jurídica a partir do marco civil da internet. **Anais do 4º Congresso Internacional de Direito e Contemporaneidade: mídias e direitos da sociedade em rede UFSM**. 2017. Disponível em: http://coral.ufsm.br/congressodireito/anais/2017/9-2.pdf. Acesso em: 22 ago. 2019.

CAVALCANTE, Jouberto de Quadros Pessoa. **Sociedade, tecnologia e a luta pelo emprego**. 1. ed. São Paulo: LTr, 2018.

CAVALCANTI, Natália Peppi; SANTOS, Luiza Mendonça da Silva Belo. A Lei Geral de Proteção de Dados do Brasil na era do *Big Data*. *In:* FERNANDES, Ricardo Vieira de Carvalho; CARVALHO, Angelo Gamba Prata de (coord.). **Tecnologia jurídica & direito digital**: II Congresso Internacional de Direito, Governo e Tecnologia – 2018. Belo Horizonte: Fórum, 2018. p. 351-366.

CHEHAB, Gustavo Carvalho. **A privacidade ameaçada de morte***:* desafios à proteção dos dados pessoais na relação de emprego pelo uso da informática. São Paulo: LTr, 2015.

CHEHAB, Gustavo Carvalho. A proteção dos dados pessoais e sensíveis do empregado. **Revista LTr**: Legislação do Trabalho. São Paulo, v. 76, n. 9, p. 1074-1083, set. 2012.

CIRIACO, Douglas. Internet é usada por 4,1 bilhões de pessoas em todo o mundo, aponta estudo. **Tecmundo**, 17 out. 2018. Disponível em: https://www.tecmundo.com.br/internet/135281-internet-usada-4-bilhoes-pessoas-mundo-aponta-estudo.htm. Acesso em: 17 ago. 2019.

COMISSÃO EUROPEIA. **Adequacy decisions**: how the EU determines if a non-EU country has an adequate level of data protection. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. Acesso em: 12 set. 2019.

COMISSÃO EUROPEIA. **Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679, de 03 de outubro de 2017**. Disponível em: https://www.cnpd.pt/bin/rgpd/docs/wp251rev01_pt.pdf. Acesso em: 23 ago. 2019.

COMISSÃO EUROPEIA. **Parecer 8/2014, de 16 de setembro de 2014.** Dispõe sobre os recentes desenvolvimentos na Internet das Coisas. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_pt.pdf. Acesso em: 08 ago. 2019.

COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS (CNPD). **Deliberação nº 1638/2013**: aplicável aos tratamentos de dados pessoais decorrentes do controlo da

utilização para fins privados das tecnologias de informação e comunicação no contexto laboral. Lisboa, Portugal: 2013. Disponível em: https://www.cnpd.pt/bin/orientacoes/Delib_controlo_comunic.pdf. Acesso em: 25 out. 2019.

COMPLIANCE TOTAL. **Pilares de um Mecanismo de Integridade e Sistema de Compliance**. Texto baseado no conteúdo do livro "Compliance - A excelência na prática" de Wagner Giovanini. 2014. Disponível em: https://www.compliancetotal.com.br/compliance/pilares. Acesso em: 14 out. 2019.

CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA (CADE). **Guia para programas de *compliance***. Brasília, 2016. Disponível em: http://www.cade.gov.br/acesso-a-informacao/publicacoes-institucionais/guias_do_Cade/guia-compliance-versao-oficial.pdf. Acesso em: 11 jan. 2019.

CONSELHO DA EUROPA. **Convenção europeia dos direitos do homem, de 04 de Novembro de 1950.** Dispõe sobre a protecção dos direitos do homem e das liberdades fundamentais. Disponível em: https://www.echr.coe.int/Documents/Convention_POR.pdf. Acesso em: 29 jul. 2019.

CONSELHO DA EUROPA. **Convenção nº 108, de 28 de Janeiro de 1981**. Dispõe sobre a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108. Acesso em: 07 set. 2018.

CONSELHO DA JUSTIÇA FEDERAL (CJF). **IV Jornada de Direito Civil**: enunciados aprovados. Brasília: CJF, 2006. Disponível em: https://www.cjf.jus.br/cjf/CEJ-Coedi/jornadas-cej/IV%20JORNADA%20DE%20DIREITO%20CIVIL%202013%20ENUNCIADOS%20APROVADOS.pdf/view. Acesso em: 07 out. 2019.

CONSELHO EUROPEU. **UE estabelece obrigações de transparência para plataformas em linha**. 14 jun. 2019. Disponível em: https://www.consilium.europa.eu/pt/press/press-releases/2019/06/14/eu-introduces-transparency-obligations-for-online-platforms/. Acesso em: 03 nov. 2019.

CUESTA, Henar Álvarez. **El futuro del trabajo vs. El trabajo del futuro**: implicaciones laborales de la industria 4.0. A Coruña: Colex, 2017.

CUEVA, Ricardo Villas Bôas. A insuficiente proteção de dados pessoais no Brasil. **Revista de Direito Civil Contemporâneo**. São Paulo: Ed. RT, ano 4, v. 13, p. 59-67, out./dez. 2017.

DACHERI, Emanueli. **O impacto da tecnologia nas relações de trabalho**: uma análise à luz da teoria da eficácia horizontal dos direitos fundamentais da personalidade dos trabalhadores. *2*019. Dissertação (Mestrado em Direito) – Universidade do Extremo Sul Catarinense, 2019.

DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS – DUDH. 1948. **Centro de**

Informações das Nações Unidas para o Brasil (UNIC Rio). Rio de Janeiro, 2009. Disponível em: https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf. Acesso em: 07 ago. 2019.

DE AMORIM, Jorge Eduardo Braz. "A 'indústria 4.0' e a sustentabilidade do modelo de financiamento do Regime Geral da Segurança Social." **Cadernos de Dereito Actual***.* Santiago de Compostela, n. 5, p. 243-254, 2017. Disponível em: http://www.cadernosdedereitoactual.es/ojs/index.php/cadernos/article/view/132/93. Acesso em: 22 jun. 2019.

DELGADO, Godinho. **Curso de direito do trabalho**. 16. ed. rev. e ampl. São Paulo: LTr, 2017.
DIÁRIO ELETRÔNICO DA JUSTIÇA DO TRABALHO (DEJT). Resolução CSJT nº 139, de 24 de junho de 2014. **Caderno Judiciário do Conselho Superior da Justiça do Trabalho**. Brasília, p. 7-8, 24 jun. 2014.

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

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: 24 jul. 2019.

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

FACCHINI NETO, Eugênio. Da responsabilidade civil no novo código. **Revista do Tribunal Superior do Trabalho**, Porto Alegre, RS, v. 76, n. 1, p. 17-63, jan./mar. 2010.

FERNANDES, Ricardo Vieira de Carvalho; CARVALHO, Angelo Gamba Prata de (coord.). **Tecnologia jurídica & direito digital**: II Congresso Internacional de Direito, Governo e Tecnologia – 2018. Belo Horizonte: Fórum, 2018.

FINCATO, Denise Pires (org.). **Novas tecnologias, processo e relações de trabalho***.* Porto Alegre: Sapiens, 2015.

FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. *Compliance* de dados pessoais. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). **A lei geral de proteção de dados pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Revista dos Tribunais, 2019. p. 677-715.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). **A lei geral de proteção de dados pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Revista dos Tribunais, 2019.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo JOBIM. **Manual de direito civil**. São Paulo: Saraiva, 2017. *E-book* (1768 p).

GIMÉNEZ, Alfonso Ortega. Cuestiones prácticas laborales en materia de protección de datos de carácter personal tras el nuevo reglamento general de protección de la datos de la UE. **Revista Española de Derecho del Trabajo**. Cizur Menor, n. 216, p. 01-31, 2019.

GOLDSCHMIDT, Rodrigo. Art. 223-A a 233-G da CLT. *In*: LISBÔA, Daniel; MUNHOZ, José Lucio (org.). **Reforma trabalhista comentada por juízes do trabalho**: artigo por artigo. 2. ed. Rev. e ampl. São Paulo: LTr, 2019a. p. 131- 141.

GOLDSCHMIDT, Rodrigo. Direitos da personalidade do trabalhador**:** aproximações conceituais e tentativa de conformação de um microssistema trabalhista. *In*: GOLDSCHMIDT, Rodrigo. **Direitos da personalidade do trabalhador.** Rio de Janeiro: Lumen Juris, 2019, p. 01-36.

GOLDSCHMIDT, Rodrigo. **Direitos da personalidade do trabalhador.** Rio de Janeiro: Lumen Juris, 2019b.

GOLDSCHMIDT, Rodrigo. **Flexibilização dos direitos trabalhistas**: ações afirmativas da dignidade da pessoa humana como forma de resistência. São Paulo: LTr, 2009.

GONZÁLEZ, Ana Belem Hernández; GAMBOA, Oscar Zavala. Datos personales en las relaciones laborales del sector privado. **Revista Latinoamericana de Derecho Social**. México, n. 27, p. 221-231, jul./dez. 2018.

GOULART, Guilherme Damasio. Limites do BYOD: entre o poder do empregador e a proteção dos direitos da personalidade do empregado. **Revista de direito do trabalho**, São Paulo, v. 40, n. 159, p. 71-86, set./out. 2014.

GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29 (GT29). **Dispõe sobre orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é "suscetível de resultar num elevado risco" para efeitos do Regulamento (UE) 2016/679.** Revistas e adotadas pela última vez em 4 de outubro de 2017a. Disponível em: https://www.cnpd.pt/bin/rgpd/docs/wp248rev.01_pt.pdf. Acesso em: 16 out. 2019.

GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29 (GT29). **Dispõe sobre orientações sobre o consentimento ao abrigo do Regulamento (UE) 2016/679**. Última redação revista e adotada em 10 de abril de 2018. Disponível em: http://www.ua.pt/file/53847. Acesso em: 17 out. 2019.

GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29 (GT29). **Dispõe sobre orientações sobre os encarregados da proteção de dados (EPD)**. Com a última redação revista e adotada em 5 de abril de 2017b. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048. Acesso em: 17 out. 2019.

GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29 (GT29). **Parecer 05/2014, de 10 de abril de 2014a**. Dispõe sobre técnicas de anonimização. Disponível em: https://www.gpdp.gov.mo/uploadfile/2016/0831/20160831042518381.pdf. Acesso em: 04 out. 2019.

GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29 (GT29). **Parecer 06/2014, de 09 de abril de 2014b**. Dispõe sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.º da Diretiva 95/46/CE. Disponível em: https://www.gpdp.gov.mo/uploadfile/2015/0803/20150803050042662.pdf. Acesso em: 04 out. 2019.

HAO, Karen. The AI gig economy is coming for you. **Mit Technology Review**, 31 maio 2019. Disponível em: https://www.technologyreview.com/s/613606/the-ai-gig-economy-is-coming-for-you/. Acesso em: 15 ago. 2019.

HARARI, Yuval Noah. **Homo Deus**: uma breve história do amanhã. Trad. Paulo Geiger. 1. ed. São Paulo: Companhia das Letras, 2016.

INSTITUTO DE PESQUISA ECONÔMICA APLICADA (IPEA). Mercado de Tabalho: conjuntura e análise. **Ministério da Economia**. Brasil, ano 25, n. 66, abr. 2019. Disponível em: http://www.ipea.gov.br/portal/index.php?option=com_content&view=article&id=34732:boletim-mercado-de-trabalho-conjuntura-e-analise-no-66&catid=184:disoc&directory=1. Acesso em: 14 jul. 2019.

JANONI, Daniella; GIEREMEK, Rogéria. **Relações de Trabalho e Compliance**: parceria necessária. São Paulo, 01 fev. 2013. Disponível em: http://www.administradores.com.br/noticias/carreira/relacoes-de-trabalho-e-compliance-parceria-necessaria/73122/. Acesso em: 26 out. 2019.

JOBIM, Rosana Kim. ***Compliance* e trabalho**: entre o poder diretivo do empregador e os direitos inespecíficos do empregado. Florianópolis: Tirant Lo Blanch, 2018.

LAZZARIN, Sonilde Kugel; CAVAGNOLI, Fernanda Onzi. *Compliance* trabalhista. **Revista Fórum Justiça do Trabalho**. Belo Horizonte, v. 35, n. 417, p. 95-110, set. 2018.

LEITE, Marcelo. Autor de 'Homo Deus' mapeia as graves implicações da tecnologia. **Folha de São Paulo**, São Paulo, 12 nov. 2016. Disponível em: https://www1.folha.uol.com.br/ciencia/2016/11/1831776-autor-de-homo-deus-mapeia-as-graves-implicacoes-da-tecnologia.shtml. Acesso em: 17 ago. 2019.

LEME, Ana Carolina Reis Paes; RODRIGUES, Bruno Alves; CHAVES JÚNIOR, José Eduardo de Resende (coord.). **Tecnologias disruptivas e a exploração do trabalho humano**. São Paulo: LTr, 2017.

LIMBERGER, Têmis. Da evolução do direito a ser deixado em paz à proteção dos dados pessoais. **Novos Estudos Jurídicos**, Itajaí, v. 14, n. 2, p. 27-53, 2º

Quadrimestre. 2009. Disponível em: https://siaiap32.univali.br/seer/index.php/nej/article/view/1767/1407. Acesso em: 10 set. 2019.

LIPOVETSKY, Gilles. **A sociedade da decepção**. Barueri: Manole, 2007.

LISBÔA, Daniel; MUNHOZ, José Lucio (org.). **Reforma trabalhista comentada por juízes do trabalho**: artigo por artigo. 2. ed. Rev. e ampl. São Paulo: LTr, 2019.

LOPES, Teresa Vale. Responsabilidade e governação das empresas no âmbito do novo regulamento sobre a proteção e dados. *In*: PEREIRA COUTINHO, Francisco; CANTO MONIZ, Graça (coord.). **Anuário da Proteção de Dados 2018**. Lisboa: CEDIS, 2018. p. 45-69.

LUCA, Cristina de. Por que é preciso incluir proteção de dados entre os direitos fundamentais. **Blog Porta 23**, 13 ago. 2019. Disponível em: https://porta23.blogosfera.uol.com.br/2019/08/13/por-que-e-preciso-incluir-protecao-de-dados-entre-os-direitos-fundamentais/. Acesso em: 14 set. 2019.

MANNRICH, Nelson. Futuro do Direito do Trabalho, no Brasil e no Mundo. **Revista LTr**: Legislação do Trabalho. São Paulo, v. 81, n. 11, p. 1287-1300, nov. 2017.

MATHIES, Anaruez. **Assédio moral e compliance na relação de emprego**: dos danos e dos custos e instrumentos de prevenção. Curitiba: Juruá, 2018. p. 131-181.

MEDEIROS, Benizete Ramos de (coord.). **O Mundo do trabalho em movimento e as recentes alterações legislativas:** um olhar luso-brasileiro. São Paulo: LTr, 2018.

MING, Celso. **O trabalho em mutação**. 15 jan. 2017. Disponível em: http://gilvanmelo.blogspot.com/2017/01/o-trabalho-em-mutacao-celso-ming.html?m=0. Acesso em: 11 jul. 2019.

MOREIRA, Teresa Alexandra Coelho. Algumas Questões sobre Trabalho 4.0. *In*: MEDEIROS, Benizete Ramos de (coord.). **O Mundo do trabalho em movimento e as recentes alterações legislativas:** um olhar luso-brasileiro. São Paulo: LTr, 2018. p. 191-201.

MOREIRA, Teresa Alexandra Coelho. **A privacidade dos trabalhadores e as novas tecnologias de informação e comunicação**: um contributo para um estudo dos limites do poder de controlo electrónico do empregador. Coimbra: Almedina. 2010.

MOREIRA, Teresa Alexandra Coelho. **Estudos de direito do trabalho**. Coimbra, Portugal: Almedina, 2016. v. 2.

MOREIRA, Teresa Alexandra Coelho. Novas tecnologias: um admirável mundo novo do trabalho? **Revista de Direitos e Garantias Fundamentais**. Vitória, n. 11, p. 15-52, jan./jun. 2012.

MUNIZ, Mirella Karen de Carvalho Bifano; DIAS, Ronaldo Mayrink de Castro Garcia. Compliance e Direito do Trabalho: novas práticas para mitigar novos riscos. **LTr Suplemento Trabalhista**. São Paulo, v. 52, n. 094, p. 529-537, nov. 2016.

MURCIA, Joaquín García; CARDO, Iván Antonio Rodríguez. La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo. **Revista Española de Derecho del Trabajo**. Cizur Menor, n. 216, p. 1-28, 2019.

NAGESH, Ashitha. Desempregados, mas felizes: as conclusões da Finlândia após o projeto de renda mínima. **BBC News Brasil**, 12 fev. 2019. Disponível em: https://www.bbc.com/portuguese/geral-47196165. Acesso em: 15 ago. 2019.

NASCIMENTO, Amauri Mascaro. **Curso de direito do trabalho:** história e teoria geral do direito do trabalho, relações individuais e coletivas do trabalho. 26. ed. São Paulo: Saraiva, 2011.

NOVAIS, Jorge Reis. **A dignidade da pessoa humana**: dignidade e direitos fundamentais. Coimbra, Portugal: Almedina, 2015. v.1, p. 167-188.

NOVAIS, Jorge Reis. **A dignidade da pessoa humana**: dignidade e inconstitucionalidade. Coimbra, Portugal: Almedina, 2016. v.2, p. 95-142.

OITAVEN, Juliana Carreiro Corbal; CARELLI, Rodrigo de Lacerda; CASAGRANDE, Cássio Luís. **Empresas de transporte, plataformas digitais e a relação de emprego**: um estudo do trabalho subordinado sob aplicativos. Brasília: Ministério Público do Trabalho, 2018.

OLIVEIRA, Ricardo Alexandre de. Lei geral de proteção de dados pessoais e seus impactos no ordenamento jurídico. **Revista dos Tribunais**, São Paulo, v. 998, p. 241-261, dez. 2018.

ORGANIZAÇÃO INTERNACIONAL DO TRABALHO (OIT). **Constituição OIT e Declaração de Filadélfia**. 1944. Disponível em: https://www.ilo.org/wcmsp5/groups/public/---americas/---ro-lima/---ilo-brasilia/documents/genericdocument/wcms_336957.pdf. Acesso em: 10 ago. 2019.

ORGANIZAÇÃO INTERNACIONAL DO TRABALHO (OIT). **Declaração da OIT sobre os Princípios e Direitos Fundamentais no Trabalho**. 1998. Disponível em: https://www.ilo.org/public/english/standards/declaration/declaration_portuguese.pdf. Acesso em: 01 nov. 2019.

ORGANIZACIÓN INTERNACIONAL DEL TRABAJO (OIT). **ILO Centenary Declaration**. Geneva: International Labour Office, 2019. Disponível em: https://www.ilo.org/wcmsp5/groups/public/---ed_norm/---relconf/documents/meetingdocument/wcms_700622.pdf. Acesso em: 03 nov. 2019.

ORGANIZACIÓN INTERNACIONAL DEL TRABAJO (OIT). **Repertorio de recomendaciones prácticas de la OIT**. Ginebra: Oficina Internacional del Trabajo,

1997. Disponível em: http://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_112625.pdf. Acesso em: 23 ago. 2018.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Legislação sobre proteção de dados e privacidade em todo o mundo***.* Disponível em: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx. Acesso em: 09 set. 2019.

ORGANIZAÇÃO DE COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). **Diretrizes da OCDE sobre a proteção da privacidade e do fluxo transfronteiriço de dados pessoais**. 1980. Disponível em: http://www.oecd.org/sti/ieconomy/15590254.pdf. Acesso em: 09 set. 2019.

OSELAME, Carolina Pedroso; GUIMARÃES, Cíntia Ione Santiago...[et al.]. (org.). **Novas tecnologias, processo e relação de trabalho** estudos em homenagem aos 20 anos de docência da professora doutora Denise Pires Fincato. Porto Alegre: Livraria do Advogado, 2019. p. 151-165.

PACTO INTERNACIONAL DOS DIREITOS CIVIS E POLÍTICOS – PIDCP. 1966. Disponível em: https://www.oas.org/dil/port/1966%20Pacto%20Internacional%20sobre%20Direitos%20Civis%20e%20Pol%C3%ADticos.pdf. Acesso em: 30 out. 2019.

PACTO INTERNACIONAL DOS DIREITOS ECONÔMICOS, SOCIAIS E CULTURAIS – PIDESC. 1966. Disponível em: https://www.oas.org/dil/port/1966%20Pacto%20Internacional%20sobre%20os%20Direitos%20Econ%C3%B3micos,%20Sociais%20e%20Culturais.pdf. Acesso em: 07 ago. 2019.

PEREIRA COUTINHO, Francisco; CANTO MONIZ, Graça (coord.). **Anuário da Proteção de Dados 2018**. Lisboa: CEDIS, 2018.

PÉREZ LUÑO, Antonio-Enrique. **Derechos Humanos, Estado de Derecho y Constituición**. 10. ed. Madrid: Editorial Tecnos, 2010.

PIERRO, Bruno de. O mundo mediado por algoritmos. **Pesquisa FAPESP**. São Paulo, ano 19, n. 266, abr. 2018. Disponível em: http://revistapesquisa.fapesp.br/2018/04/19/folheie-a-edicao-266/. Acesso em: 05 set. 2019.

PINHEIRO, Patrícia Peck Garrido. Nova lei brasileira de proteção de dados pessoais (LGPD) e o impacto nas instituições públicas e privadas. Sociedade da informação: inquietudes e desafios. **Revista dos Tribunais***,* São Paulo, v. 1000, ano 108, p. 309-323, fev. 2019.

POMBO, Olga. Panóptico. **Faculdade de Ciências da Universidade de Lisboa.** Disponível em: http://www.educ.fc.ul.pt/docentes/opombo/hfe/momentos/sociedade%20disciplinar/Pan%C3%B3ptico.htm. Acesso em: 06 set. 2019.

PORTUGAL. **Constituição da República Portuguesa de 1976**. Disponível em: https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx. Acesso em: 27 jul. 2019.

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

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. O direito à proteção dos dados pessoais: uma leitura do sistema europeu e a necessária tutela dos dados sensíveis como paradigma para um sistema jurídico brasileiro. **Revista Brasileira de Direitos Fundamentais & Justiça**. Programa de Pós-Graduação Mestrado e Doutorado em Direito da PUCRS. Porto Alegre, ano 4, n. 11, p. 162-180, abr./jun. 2010.

RUBIO, Isabel. Amazon prescinde de una inteligencia artificial de reclutamiento por discriminar a las mujeres. **El País**, 12 out. 2018. Disponível em: https://elpais.com/tecnologia/2018/10/11/actualidad/1539278884_487716.html. Acesso em: 16 mar. 2019.

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

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 11. ed. rev. e atual. Porto Alegre: Livraria do Advogado, 2012. *E-Book*.

SARLET, Ingo Wolfgang; MELLO FILHO, Luiz Philippe de; FRAZÃO, Ana de Oliveira. (coord.). **Diálogos entre o direito do trabalho e o direito constitucional**: estudos em homenagem a Rosa Maria Weber. São Paulo: Saraiva, 2014.

SCHREIBER, Anderson. **Direitos da personalidade**. 2. ed. São Paulo: Atlas, 2013.

SCHREIBER, Anderson. PEC 17/2019: uma análise crítica. **Jornal Carta Forense**, 18 jul. 2019. Disponível em: http://cartaforense.com.br/conteudo/colunas/pec-1719-uma-analise-critica/18345. Acesso em: 14 set. 2019.

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: 03 set. 2019.

SCHWAB, Klaus. **A quarta revolução industrial**. São Paulo: Edipro, 2016.

SENADO NOTÍCIAS. Proteção de dados pessoais deverá ser direito fundamental na Constituição. **Senado Federal**, 02 jul. 2019. Disponível em: https://www12.senado.leg.br/noticias/materias/2019/07/02/protecao-de-dados-pessoais-devera-entrar-na-constituicao-como-direito-fundamental. Acesso em: 06 jul. 2019.

SIGNES, Adrián Todolí. El futuro del trabajo: nuevos indicios de la laboralidad aplicables a empresas digitales. **Revista de Treball, Economia I Societat**, n. 92, p. 1-8, enero 2019. Disponível em: http://www.ces.gva.es/sites/default/files/2019-02/art9_3.pdf. Acesso em: 06 jun. 2019.

SIGNES, Adrián Todolí. La evalución de los trabajadores por parte de los clientes como método de vigilancia y control en la emrpesa: reputación *online* y protección de datos. **RTSS.CEF**, n. 427, p. 63-90, out. 2018.

SIGNES, Adrián Todolí. O Mercado de Trabalho no século XXI: *on-demandeconomy*, *crowdsourcing* e outras formas de descentralização produtiva que atomizam o mercado de trabalho. Tradução Ana Carolina Reis Paes Leme e Carolina Rodrigues Carsalade. *In*: LEME, Ana Carolina Reis Paes; RODRIGUES, Bruno Alves; CHAVES JÚNIOR, José Eduardo de Resende (coord.). **Tecnologias disruptivas e a exploração do trabalho humano**. São Paulo: LTr, 2017. p. 28-43.

SILVA, José Afonso da. **Aplicabilidade das normas constitucionais**. 5. ed. São Paulo: Malheiros, 2001.

SILVA, Rosane Leal da. A publicação de decisões nos portais dos Tribunais trabalhistas e a vulnerabilidade dos dados pessoais dos empregados. *In*: OSELAME, Carolina Pedroso; GUIMARÃES, Cíntia Ione Santiago...[et al.]. (org.). **Novas tecnologias, processo e relação de trabalho** estudos em homenagem aos 20 anos de docência da professora doutora Denise Pires Fincato. Porto Alegre: Livraria do Advogado, 2019. p. 151-165.

SILVA, Virgílio Afonso da. **A constitucionalização do direito**: os direitos fundamentais nas relações entre particulares. 1. ed. São Paulo: Malheiros, 2011.

SIMÓN, Sandra Lia. **A proteção constitucional da intimidade e da vida privada do empregado***.* São Paulo: LTr, 2000.

SOLÍS, Julio Ismael Camacho. **El trabajo digital 4.0**. 2019. Disponível em: http://www.cielolaboral.com/el-trabajo-digital-4-0/. Acesso em: 13 jul. 2019.

STIVAL, Juliane. O anteprojeto brasileiro de lei de proteção dos dados pessoais e os dados dos Trabalhadores na relação laboral. *In*: FINCATO, Denise Pires (org.). **Novas tecnologias, processo e relações de trabalho***.* Porto Alegre: Sapiens, 2015. p. 129-145.

SUPIOT, Alain. Lei e trabalho. Um mercado mundial de regras? Tradução Rinaldo José Varussa. **Tempos Históricos**, v. 17, p. 157-169, 2013. Disponível em: http://e-revista.unioeste.br/index.php/temposhistoricos/article/view/9013. Acesso em: 17 jul. 2019.

TEDEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Revista dos Tribunais, 2019.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. *In*: TEDEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Revista dos Tribunais, 2019. p. 287-322.

TRIBUNAL SUPERIOR DO TRABALHO (TST). **Recurso de Revista 28140-17.2004.5.03.0092**. Relator: Min. Mauricio Godinho Delgado, 10 de março de 2010. Disponível em: http://aplicacao4.tst.jus.br/consultaProcessual/consultaTstNumUnica.do?consulta=Consultar&conscsjt=&numeroTst=28140&digitoTst=17&anoTst=2004&orgaoTst=5&tribunalTst=03&varaTst=092&submit=Consultar. Acesso em: 24 ago. 2019.

TRIBUNAL SUPERIOR DO TRABALHO (TST). TST define regras sobre exigência de antecedentes criminais em julgamento de recurso repetitivo. **Secretaria de Comunicação Social do TST**, 26 abr. 2017. Disponível em: http://www.tst.jus.br/noticia-destaque/-/asset_publisher/NGo1/content/id/24287126. Acesso em: 06 out. 2019.

UNIÃO EUROPEIA. **Carta dos direitos fundamentais da União Europeia, de 7 de dezembro de 2000.** Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN. Acesso em: 10 ago. 2019.

UNIÃO EUROPEIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995**. Relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=PT. Acesso em: 28 ago. 2019.

UNIÃO EUROPEIA. **Directiva 97/66/CE do Parlamento Europeu e do Conselho, de 15 de Dezembro de 1997**. Relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das telecomunicações. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31997L0066&from=PT. Acesso em: 09 set. 2019.

UNIÃO EUROPEIA. **Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002**. Relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32002L0058&from=PT. Acesso em: 09 set. 2019.

UNIÃO EUROPEIA. **Directiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de Março de 2006**. Relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva 2002/58/CE. Disponível em https://eur-lex.europa.eu/legal-

content/PT/TXT/HTML/?uri=CELEX:32006L0024&from=PT. Acesso em: 09 set. 2019.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=pt. Acesso em: 03 set. 2019.

UNIÃO EUROPEIA. **Regulamento do Parlamento Europeu e do Conselho**. Relativo à promoção da equidade e da transparência para os utilizadores profissionais de serviços de intermediação em linha. Disponível em: https://data.consilium.europa.eu/doc/document/PE-56-2019-INIT/pt/pdf. Acesso em: 04 nov. 2019.

UNITED NATIONS. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. **General Assembly**, 16 maio 2011. Disponível em: https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf. Acesso em: 18 ago. 2019.

VECCHI, Ipojucan Demétrius. A eficácia dos direitos fundamentais nas relações privadas: o caso da relação de emprego. **Revista do TST**, Brasília, v. 77, n. 3, p. 111-135, jul./set. 2011.

WEINSCHENKER, Marina Santoro Franco. **A vida laboral e extralaboral do empregado**: a privacidade no contexto das novas tecnologias e dos direitos fundamentais. São Paulo: LTr, 2013.

WOLKMER, Antonio Carlos. Direitos humanos: novas dimensões e novas fundamentações. **Direito em debate**, ano X, n. 16/17, p. 9-32, jan./jun. 2002.

WORLD ECONOMIC FORUM. The Future of Jobs Employment, Skills and Workforce Strategy for the Fourth Industrial Revolution. **Weforum**. Suíça, jan. 2016. Disponível em: https://drive.google.com/file/d/15UFtX0Ly5_VWUj-VPBRN3n6uR3bkW8QQ/view. Acesso em: 16 jun. 2019.

WORLD ECONOMIC FORUM. The Global Risks Report 2019. **Weforum**. Suíça, 2019. Disponível em: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf. Acesso em: 06 set. 2019.